S. HRG. 115–418

FOREIGN CYBER THREATS TO THE UNITED STATES

HEARING

BEFORE THE

COMMITTEE ON ARMED SERVICES UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

JANUARY 5, 2017

Printed for the use of the Committee on Armed Services

Available via the World Wide Web: http://www.Govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
33–940 PDF WASHINGTON : 2019

COMMITTEE ON ARMED SERVICES

JOHN MCCAIN, Arizona, *Chairman*

JAMES M. INHOFE, Oklahoma	JACK REED, Rhode Island
ROGER F. WICKER, Mississippi	BILL NELSON, Florida
DEB FISCHER, Nebraska	CLAIRE MCCASKILL, Missouri
TOM COTTON, Arkansas	JEANNE SHAHEEN, New Hampshire
MIKE ROUNDS, South Dakota	KIRSTEN E. GILLIBRAND, New York
JONI ERNST, Iowa	RICHARD BLUMENTHAL, Connecticut
THOM TILLIS, North Carolina	JOE DONNELLY, Indiana
DAN SULLIVAN, Alaska	MAZIE K. HIRONO, Hawaii
DAVID PERDUE, Georgia	TIM KAINE, Virginia
TED CRUZ, Texas	ANGUS S. KING, JR., Maine
LINDSEY GRAHAM, South Carolina	MARTIN HEINRICH, New Mexico
BEN SASSE, Nebraska	ELIZABETH WARREN, Massachusetts
LUTHER STRANGE, Alabama	GARY C. PETERS, Michigan

CHRISTIAN D. BROSE, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

CONTENTS

JANUARY 5, 2017

FOREIGN CYBER THREATS TO THE UNITED STATES

THURSDAY, JANUARY 5, 2017

U.S. SENATE,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The committee met, pursuant to notice, at 9:29 a.m. in Room SD–G50, Dirksen Senate Office Building, Senator John McCain (chairman) presiding.

Committee members present: Senators McCain, Inhofe, Wicker, Fischer, Cotton, Rounds, Ernst, Tillis, Sullivan, Graham, Cruz, Reed, Nelson, McCaskill, Shaheen, Gillibrand, Blumenthal, Donnelly, Hirono, Kaine, King, and Heinrich.

Other Senators Present: Senators Purdue, Warren, Peters, and Sasse.

OPENING STATEMENT OF SENATOR JOHN MCCAIN, CHAIRMAN

Chairman MCCAIN. Well, good morning, everyone.

Before we begin, I want to welcome all our members back to the committee and extend a special welcome to the new members joining us. On the Republican side, we are joined by Senator Purdue and Senator Sasse. On the Democrat side, we are joined by Senator Warren and Senator Peters.

It is a special privilege to serve on this committee, most of all because it affords us the opportunity to spend so much time in the company of heroes, the men and women who serve and sacrifice on our behalf every day. I hope you will come to cherish your service on this committee as much as I have over the years, and I look forward to working with each of you.

The committee meets this morning for the first in a series of hearings on cybersecurity to receive the testimony on foreign cyber threats to the United States. I would like to welcome our witnesses this morning: James Clapper, Director of National Intelligence; Marcel Lettre, Under Secretary of Defense for Intelligence; and Admiral Mike Rogers, Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service.

This hearing is about the range of cybersecurity challenges confronting our Nation, threats from countries like Russia, China, and North Korea and Iran, as well as non-state actors from terrorist groups to transnational criminal organizations. In recent years, we have seen a growing series of cyber attacks by multiple actors, attacks that have targeted our citizens, businesses, military, and government. But there is no escaping the fact that this committee

meets today for the first time in this new Congress in the aftermath of an unprecedented attack on our democracy.

At the President's direction, Director Clapper is leading a comprehensive review of Russian interference in our recent election with the goal of informing the American people as much as possible about what happened. I am confident that Director Clapper will conduct this review with the same integrity and professionalism that has characterized his nearly half a century of government and Military Service. I am equally confident in the dedicated members of our intelligence community.

The goal of this review, as I understand it, is not to question the outcome of the presidential election. Nor should it be. As both President Obama and President-elect Trump have said, our Nation must move forward. But we must do so with full knowledge of the facts. I trust Director Clapper will brief the Congress on his review when it is completed. This is not the time or place to preview its findings.

That said, we know a lot already. In October, our intelligence agencies concluded unanimously that, quote, the Russian Government directed compromises of emails from United States persons and institutions, including from United States political organizations. They also assessed that, quote, disclosures of alleged hacked emails were consistent with the methods and motivations of Russian-directed efforts and that these thefts and disclosures were intended to interfere with the United States election process.

Since then, our intelligence community has released additional information concerning these Russian activities, including a joint analysis report that provided technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence services to attack the United States.

Every American should be alarmed by Russia's attacks on our Nation. There is no national security interest more vital to the United States of America than the ability to hold free and fair elections without foreign interference. That is why Congress must set partisanship aside, follow the facts, and work together to devise comprehensive solutions to deter, defend against and, when necessary, respond to foreign cyber attacks.

As we do, we must recognize that the recent Russian attacks are one part of a much bigger cyber problem. Russian cyber attacks have targeted the White House, the Joint Staff, the State Department, our critical infrastructure. Chinese cyber attacks have reportedly targeted NASA, the Departments of State and Commerce, congressional offices, military labs, the Naval War College, and United States businesses, including major defense contractors. Most recently, China compromised over 20 million background investigations at the Office of Personnel Management. Iran has used cyber tools in recent years to attack the United States Navy, United States partners in the Middle East, major financial institutions, and a dam just 25 miles north of New York City. Of course, North Korea was responsible for the massive cyber attack on Sony Pictures in 2014.

What seems clear is that our adversaries have reached a common conclusion: that the reward for attacking America in cyberspace outweighs the risk. For years, cyber attacks on our Nation have

been met with indecision and inaction. Our Nation has no policy and thus no strategy for cyber deterrence. This appearance of weakness has been provocative to our adversaries who have attacked us again and again with growing severity. Unless we demonstrate that the costs of attacking the United States outweigh the perceived benefits, these cyber attacks will only grow.

This is also true beyond the cyber domain. It should not surprise us that Vladimir Putin would think he could launch increasingly severe cyber attacks against our Nation when he has paid little price for invading Ukraine, annexing Crimea, subverting democratic values and institutions across Europe, and of course, helping Bashar Assad slaughter civilians in Syria for more than a year with impunity. The same is true for China, Iran, North Korea, and any other adversary that has recently felt emboldened to challenge the world order. Put simply, we cannot achieve cyber deterrence without restoring the credibility of United States deterrence more broadly.

To do so, we must first have a policy, which means finally resolving the long list of basic cyber questions that we as a Nation have yet to answer. What constitutes an act of war or aggression in cyberspace that would merit a military response, be it by cyber or other means? What is our theory of cyber deterrence, and what is our strategy to implement it? Is our Government organized appropriately to handle this threat, or are we so stove-piped that we cannot deal with it effectively? Who is accountable for this problem, and do they have sufficient authorities to deliver results? Are we in the Congress just as stove-piped on cyber as the executive branch such that our oversight actually reinforces problems rather than helping to resolve them? Do we need to change how we are organized?

This committee intends to hold a series of hearings in the months ahead to explore these and other questions. We look forward to hearing the candid views of our distinguished witnesses today who have thought about and worked on these questions as much as anyone in our Nation.

Senator Reed?

STATEMENT OF SENATOR JACK REED

Senator REED. Well, thank you very much, Mr. Chairman. I want to commend you for your leadership in promptly scheduling this hearing on foreign cyber threats.

I would also like to welcome our witnesses: Director Clapper, Under Secretary Lettre, and Admiral Rogers. Thank you, gentlemen, for your service and your dedication.

While I understand that our witnesses will be discussing the cyber threats that many countries, including China and India, pose to our Nation, I would like to focus for a few minutes on the widely reported instances of Russian hacking and disinformation that raised concerns regarding the election of 2016.

In addition to stealing information from the Democratic National Committee and the Clinton campaign and cherry-picking what information it leaked to the media, the Russian Government also created and spread fake news and conspiracies across the vast social media landscape. At the very least, the effect of Russia's actions

was to erode the faith of the American people in our democratic institutions. These and other cyber tools remain highly active and engaged in misinforming our political dialogue even today.

There is still much we do not know, but Russia's involvement in these intrusions does not appear to be in any doubt. Russia's best cyber operators are judged to be as elusive and hard to identify as any in the world. In this case, however, detection and attribution were not so difficult, the implication being that Putin may have wanted us to know what he had done, seeking only a level of plausible deniability to support an official rejection of culpability.

These Russian cyber attacks should be judged within the larger context of Russia's rejection of the post-Cold War international order and aggressive actions against its neighbors. Russia's current leaders, and President Putin in particularly, perceive the democratic movements in the former Soviet states, the West's general support for human rights, press freedoms, the rule of law and democracy, as well as NATO and EU enlargement, as a threat to what they believe is Russia's sphere of influence.

Putin's Russia makes no secret of the fact that it is determined to aggressively halt and counter what it characterizes as Western encroachment on its vital interests. The invasion of Georgia, the annexation of Crimea, the aggression against Ukraine featuring sophisticated hybrid warfare techniques, the continuing military buildup despite a declining economy, saber-rattling in the Baltics and Baltic Sea, the authoritarian onslaught against the press, NGOs, and what remains of the Russian democratic opposition, the unwavering campaign for national sovereignty over the Internet, and the creation of an "iron information curtain" like China's Great Firewall and its aggressive interference in Western political processes all are of one piece. Russia's efforts to undermine democracy at home and abroad and destabilize the countries on its border cannot be ignored or traded away in exchange for the appearance of comity.

Furthermore, what Russia did to the United States in 2016, it has already done and continues to do in Europe. This challenge to the progress of democratic values since the end of the Cold War must not be tolerated.

Despite the indifference of some to this matter, our Nation needs to know in detail what the intelligence community has concluded was an assault by senior officials of a foreign government on our electoral process.

Our electoral process is the bedrock of our system of government. An effort to manipulate it, especially by a regime with values and interests so antithetical to our own, is a challenge to the Nation's security which much be met with bipartisan and universal condemnation, consequences, and correction.

I believe the most appropriate means to conduct an inquiry is the creation of a special select committee in the Senate, since this issue and the solutions to the problems it has exposed spill across the jurisdictional divides of the standing committees on Armed Services, Intelligence, Foreign Relations, Homeland Security, and Judiciary. Failing that, our committee must take on as much of this task as we can, and I again commend the chairman for his commitment to do so.

Therefore, I am pleased and grateful that his efforts will be extended, the energy will be invested on the matters that are so critical to the American people. I also want to applaud President Obama's initial steps publicized last week to respond to Russia's hostile actions.

General Clapper, Under Secretary Lettre, Admiral Rogers, we appreciate your urgent efforts to discover what happened and why and to make these facts known to the President, the President-elect, Congress, and the American people. Although your investigation and report to President Obama is not yet public, we hope you will be able to convey and explain what has been accomplished so far, including the steps already announced by the President.

In addition, I am sure we will have many questions about how we are organized in the cyber domain and what changes you have recommended going forward, subjects that President Obama referenced in his signing statement of the National Defense Authorization Act for Fiscal Year 2017.

These are difficult issues, but they are of vital importance to our Nation, our security, and our democracy. Mr. Chairman, I look forward to working with you in a bipartisan manner to conduct a thorough and thoughtful inquiry and to do more to address the cyber threats our Nation faces more broadly by state and non-state actors. Thank you very much.

Chairman MCCAIN. Welcome to the witnesses, and Mr. Secretary, we will begin with you for any opening statements or comment you might have.

STATEMENT OF HONORABLE MARCEL J. LETTRE II, UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

Mr. LETTRE. Thank you, Chairman, Ranking Member Reed, members of the committee. I appreciate the opportunity to be here today. I will shortly turn the microphone over to Director Clapper for some comments, followed by Admiral Rogers. As this is my last appearance before this committee before stepping down from 8 years of Pentagon service in a few weeks, I want to——

Chairman MCCAIN. I am sure you will regret not having that opportunity again.

[Laughter.]

Mr. LETTRE. It will be nice to be skiing a little bit in February. That is for sure.

But having said that, since I am just a few weeks from stepping down, I do want to thank this committee for its partnership and I want to thank Director Clapper and Admiral Rogers for the privilege of being able to serve together with them in the leadership of the U.S. intelligence community. To the men and women of the U.S. intelligence community, civilian and military, thousands of whom are deployed today around the world advancing U.S. interests and protecting America, I do admire your integrity. I admire your service. It has been an honor to serve with you over the last many years.

In the interest of time, I will briefly note the Department of Defense's views on cyber in three core themes: first, the threats we must address; second, what we are doing to address them now; and third, the difficult but urgent work we know still lies ahead.

First, the threats. As you know, the Department of Defense's leadership believes we confront no fewer than five immediate but also distinct and evolving challenges across all operating domains. We are countering the prospect of Russian aggression and coercion, especially in Europe, something we unfortunately we have had to energetically renew our focus on in the last several years.

We are also managing historic change in perhaps the most consequential region for America's future, the Asia-Pacific, and watching for risks associated with China's destabilizing actions in the region.

We are checking Iranian aggression and malign influence across the Middle East.

We are strengthening our deterrent and defense forces in the face of North Korea's continued nuclear and missile provocations.

We are countering terrorism with the aim of accelerating the lasting defeat of ISIL [Islamic State of Iraq and the Levant] and al Qaeda.

These are what many in the Department of Defense have termed the Four Plus One, four state-based challenges and an ongoing condition of battling terrorism.

As our joint written statement for the record has detailed, each of these security challenges, China, Russia, Iran, North Korea, and global terrorist groups such as ISIL, presents a significant cyber threat dimension to the United States military. Cyber is an operating domain that is real, complex, dynamic, contested, and must be addressed.

Second, what we are doing about it. The Department of Defense has for several years pursued a comprehensive strategy for maintaining the necessary strategic dominance in this domain. Secretary of Defense Ash Carter has pressed for DOD [Department of Defense] to change, to adapt, and to innovate not only to meet today's challenges but also to ensure that we effectively defend against cyber threats well into an uncertain future.

We have built and continue to build the means and methods that will strengthen our relative position against each of these dimensions of the cyber threat. The Government cyber policies, reflected in presidential policy directives and executive orders, provide guidance on the absolute necessity of a whole-of-government approach critical to protecting our Nation.

The Department has developed, refined, and published its cyber strategy which clearly lays out three key DOD cyber missions: defending DOD networks, providing cyber options for our military commanders, and when called upon by our Nation's leaders, defending the Nation against cyber attacks of significant consequence.

As the Director and Admiral Rogers will note, since 2009, the Department has matured Cyber Command to ensure clear command responsibility and authority and growing capabilities essential to our unity of effort for cyber operations.

We also continue to mature our cyber mission forces which this fall achieved initial operating capability, or IOC, status. This force is providing military capability to execute our three missions in cyberspace. We are building new capabilities and new tools for the cyber mission force to use.

Third, what remains to be done. As much as we have done, we recognize there is much more to do. Let me mention just a couple of those most important tasks here.

First, we need to continue to develop and refine our national cyber policy framework, which includes the evolution of all dimensions of our deterrence posture: the ability to deny the adversary's objectives, to impose costs, and to ensure that we have a resilient infrastructure to execute a multi-domain mission. This refinement in evolution in our deterrent thinking and capability will further empower decision-making at net speed.

Second, within the Department, Cyber Command has matured and is doing more to protect the Nation and support global operations than ever before, and we need to continue, in fact, accelerate this maturation. Accordingly, the Secretary of Defense supports the elevation of Cyber Command to a unified combatant command and supports ending the dual hat arrangement for the leadership of NSA [National Security Administration] and Cyber Command and doing so through a deliberate conditions-based approach while continuing to leverage the shared capabilities and synergies.

Finally, we must redouble our efforts to deepen partnerships between government and the private sector and between the U.S. Government and our allies. We must continue to seek help from American industry, the source of much of the world's greatest technology talent, in innovating to find cyber defense solutions, build resiliency into our critical infrastructure systems, and strengthen our deterrence. With our international allies and partners, we must work together to promote stability in cyberspace, universal recognition that existing international law applies in cyberspace, and the adoption of voluntary peacetime norms of responsible state behavior.

Mr. Chairman, thanks. I look forward to your questions. I will now pass the baton to Director Clapper. Thank you.

Chairman MCCAIN. General Clapper?

STATEMENT OF HONORABLE JAMES R. CLAPPER, JR., DIRECTOR OF NATIONAL INTELLIGENCE

Director CLAPPER. Chairman McCain, Ranking Member Reed, and distinguished members of the committee, first thanks very much for your opening statements. Obviously, we are here today to talk about cyber threats that face our Nation, and I will offer some brief valedictory recommendations and a few parting observations. I certainly want to take note of and thank the members of the committee who are engaged on this issue and have spoken to it publicly.

I know there is a great interest in the issue of Russian interference in our electoral process based on the many classified briefings the intelligence community has already provided on this topic to the Congress. Secretary of Homeland Security Jeh Johnson and I have issued statements about it. The joint analysis report that you alluded to publicly issued by the Department of Homeland Security and the Federal Bureau of Investigation provided details on the tools and infrastructure used by the Russian intelligence services to compromise infrastructure associated with the election, as

well as a range of United States Government political and private sector entities, as you described.

As you also noted, the President tasked the intelligence community to prepare a comprehensive report on Russian interference in our election. We plan to brief the Congress and release an unclassified version of this report to the public early next week with due deference to the protection of highly sensitive and fragile sources and methods. But until then, we are really not prepared to discuss this beyond standing by our earlier statements. We are prepared to talk about other aspects of the Russian cyber threat.

We also see cyber threats challenging public trust and confidence in information services and institutions. Russia has clearly assumed an even more aggressive cyber posture by increasing cyber espionage operations, leaking data stolen from these operations, and targeting critical infrastructure systems.

China continues to succeed in conducting cyber espionage against the United States Government, our allies, and United States companies. The intelligence community and the security experts, however, have observed some reduction in cyber activities from China against United States companies since the bilateral September 2015 commitment to refrain from espionage for commercial gain.

Iran and North Korea continue to improve their capabilities to launch disruptive or destructive cyber attacks to support their political objectives.

Non-state actors, notably terrorist groups most especially including ISIL, also continue to use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by disciples, and coordinate operations. In this regard, I want to foot stomp a few points that I have made here before.

Rapidly advancing commercial encryption capabilities have had profound effects on our ability to detect terrorists and their activities. We need to strengthen the partnership between government and industry and find the right balance to enable the intelligence community and law enforcement both to operate, as well as to continue to respect the rights to privacy.

Cyber operations can also be a means to change, manipulate, or falsify electronic data or information to compromise its integrity. Cyberspace can be an echo chamber in which information, ideas, or beliefs, true or false, get amplified or reinforced through constant repetition. All these types of cyber operations have the power to chip away at public trust and confidence in our information, services, and institutions.

By way of some observations and recommendations, both the Government and the private sector have done a lot to improve cybersecurity, and our collective security is better but it is still not good enough. Our Federal partners are stepping up their efforts with the private sector but sharing what they have remains uneven. I think the private sector needs to up its game on cybersecurity and not just wait for the Government to provide perfect warning or a magic solution.

We need to influence international behavior in cyberspace. This means pursuing more global diplomatic efforts to promulgate norms of behavior in peacetime and to explore setting limits on cyber operations against certain targets.

When something major happens in cyberspace, our automatic default policy position should not be exclusively to counter cyber with cyber. We should consider all instruments of national power. In most cases to date, non-cyber tools have been more effective at changing our adversaries' cyber behavior. When we do choose to act, we need to model the rules we want others to follow since our actions set precedents.

We also need to be prepared for adversary retaliation, which may not be as surgical, either due to our adversary's skill or the inherent difficulty in calibrating effect and impact of cyber tools. That is why using cyber to counter cyber attacks risks unintended consequences.

We currently cannot put a lot of stock, at least in my mind, in cyber deterrence. Unlike nuclear weapons, cyber capabilities are difficult to see and evaluate and are ephemeral. It is accordingly very hard to create the substance and psychology of deterrence in my view.

We also have to take some steps now to invest in the future. We need to rebuild trusted working relationships with industry and the private sector on specific issues like encryption and the roles and responsibilities for government, users, and industry.

I believe we need to separate NSA and CYBERCOM [Cyber Command]. We should discontinue the temporary dual hat arrangement, which I helped design when I was Under Secretary of Defense for Intelligence 7 years ago. This is not purely a military issue. I do not believe it is in the NSA's or the IC's [intelligence community] long-term best interest to continue the dual hat setup.

Third, we must hire, train, and retain enough cyber talent and appropriately fuse cyber as a whole-of-IC workforce. Clearly cyber will be a challenge for the U.S., the intelligence community, and our national security for the foreseeable future, and we need to be prepared for that. Adversaries are pushing the envelope since this is a tool that does not cost much and sometimes is hard to attribute.

I certainly appreciate, as we all do, the committee's interest in this difficult and important challenge.

I will wrap up by saying after 53 years in the intelligence business in one capacity or another, happily I have just got 15 days left.

[Laughter.]

Director CLAPPER. I will miss being involved in the intelligence mission, and I will certainly miss the talented and dedicated patriots who are in the United States intelligence community. I am very proud of the community of professionals I have represented here for the last 6-½ years who do not get much public recognition and who like it that way. They have always supported me and I am confident they will do no less for my successor, whoever that turns out to be.

With that, let me stop and pass to Admiral Rogers.

Chairman MCCAIN. Thank you, General.

Admiral Rogers?

STATEMENT OF ADMIRAL MICHAEL S. ROGERS, USN, COMMANDER, UNITED STATES CYBER COMMAND; DIRECTOR, NATIONAL SECURITY AGENCY; CHIEF, CENTRAL SECURITY SERVICES

Admiral ROGERS. Chairman McCain, Ranking Member Reed, members of the committee, good morning and thank you for the opportunity to appear before the committee today on behalf of the United States Cyber Command and the National Security Agency.

I am honored to appear beside Director Clapper and Under Secretary Lettre and I applaud them both for their many years of public service. It has been a true honor, gentlemen.

When we last met in September, I discussed the changing cyber threat environment, and today I look forward to further discussing this complex issue. Of course, some aspects of what we do must remain classified to protect our Nation's security. Today I will limit my discussion to those in the public domain.

We have seen over the course of the last year how this cyber threat environment is constantly evolving. We have all come to take for granted the interconnectivity that is being built into every facet of our lives. It creates opportunities and vulnerabilities. Those who would seek to harm our fellow Americans and our Nation utilize the same Internet, the same communications devices, and the same social media platforms that we, our families and our friends here and around the world use. We must keep pace with such changes in order to provide policymakers and our operational commanders the intelligence and cyber capabilities they need to keep us safe. That means understanding our adversaries to the best of our ability and understanding what they mean to do and why. We are watching sophisticated adversaries involved in criminal behavior, terrorism planning, malicious cyber activities, and even outright cyber attacks. While this is a global problem, we have also recently witnessed the use of these tactics here at home.

The statement for the record that we have provided jointly to this committee covers the threat picture worldwide, but I know this hearing today will inevitably focus on reports of interference in our recent elections. I echo Director Clapper in saying that we will await the findings of the just-completed intelligence review ordered by the President and defer our comments on its specifics until after that review is shared with our leaders and congressional overseers.

I do want to add, however, that over this last year, NSA and Cyber Command have worked extensively with our broader government partners to detect and monitor Russian cyber activity. The hacking of organizations and systems belonging to our election process is of great concern, and we will continue to focus strongly on this activity.

For NSA's part, we focus on the foreign threat actor in foreign spaces, but we share our information as readily as possible with the rest of our partners in the Department of Defense, the intelligence community, and Federal law enforcement, as well as others within the U.S. Government and the private sector.

As you know, Russian cyber groups have a history of aggressively hacking into other countries' government infrastructure and even election systems. As I have indicated, this will remain a top priority for NSA and U.S. Cyber Command.

In this changing threat environment, I would like to take this opportunity to emphasize the importance of improving cybersecurity and working related issues across public and private sectors. We continue to engage with our partners around the world on what is acceptable and unacceptable behavior in cyberspace, and we clearly are not where we want to be, nor where we need to be in this regard.

We continue to make investments in technologies and capabilities to improve detection of malicious cyber activities and make it more difficult for malicious cyber actors intending to do us harm. Combating cyber threats take more than technology. It takes talented, motivated people, and we are investing more than ever in the recruitment and retention of a skilled workforce that is knowledgeable, passionate, and dedicated to protecting the Nation for the safety of our citizens and of our friends and allies around the world.

Innovation is one of the key tenets of NSA and Cyber Command and we need to invigorate the cyber workforce that think creatively about challenges that do not ascribe to traditional understandings of borders and boundaries. This remains a key driver and a key challenge as we look to the future.

Cyber Command is well along in building our cyber mission force, deploying teams to defend the vital networks that support DOD operations, to support combatant commanders in their missions worldwide, and to bolster DOD's capacity and capabilities to defend the Nation against cyber attacks of significant consequence.

The organizations I lead, the U.S. Cyber Command and the National Security Agency, have provided intelligence, expert advice, and tailored options to the Nation's decision-makers in response to recent events. Much of their activity can only be discussed in classified channels, but I must say I am proud of what both organizations have accomplished and will accomplish, even as we acknowledge we have to do more.

I look forward to your questions.

Finally, on one personal note, I apologize to all of you. I have an ongoing back issue, and if I have to stand up in the course of this time period, please do not take that as a sign of disrespect in any way. I guess I am just getting older.

That is all I have for you, sir.

Chairman MCCAIN. I know how you feel.

[Laughter.]

[The joint prepared statement of Director Clapper, Mr. Lettre, and Admiral Rogers follows:]

JOINT PREPARED STATEMENT BY THE HONORABLE JAMES R. CLAPPER, THE HONORABLE MARCEL LETTRE AND ADMIRAL MICHAEL S. ROGERS

INTRODUCTION

Chairman McCain, Vice Chairman Reed, and Members of the Committee thank you for the invitation to offer the testimony of the Department of Defense and the Intelligence Community on cyber threats to U.S. national security. Our statement reflects the collective insights of the Intelligence Community's extraordinary men and women whom we are privileged to lead. We in the Intelligence Community are committed every day to provide the nuanced, multidisciplinary intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

The order of the topics presented in this statement does not necessarily indicate the relative importance or magnitude of the threat in the view of the Intelligence Community.

Information available as of 1 January 2017 was used in the preparation of this assessment.

JOINT STATEMENT FOR THE RECORD

Information and communication technologies play an increasing role in the security of the United States. Cyberspace is both a resource on which our continued security and prosperity depends, and a globally contested medium within which threats manifest themselves. As their cyber capabilities grow, our adversaries are demonstrating a willingness to use cyberspace as a platform for espionage, attack, and influence. Foreign Intelligence Entities continue to quietly exploit our nation's public and private sectors in the pursuit of policy and military insights sensitive research, intellectual property, trade secrets, and personally identifiable information.

Cyber threats have already challenged public trust and confidence in global institutions, governance, and norms, while imposing costs on the global economy. These threats pose an increasing risk to public safety, as cyber technologies are integrated with critical infrastructure in key sectors. Adversaries also continue to use cyber operations to undermine U.S. military and commercial advantage by hacking into U.S. defense industry and commercial enterprises. The breadth of cyber threats posed to U.S. national and economic security has become increasingly diverse, sophisticated, and serious, leading to physical, security, economic, and psychological consequences.

Despite ever-improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years to come from remote hacking to establish persistent covert access, supply chain operations that insert compromised hardware or software, malicious actions by trusted insiders, and mistakes by system users. In short, the cyber threat cannot be eliminated. Rather, cyber risk must be managed in the context of overall business and operational risk. At present, however, the risk calculus some private and public sector entities employ does not adequately account for foreign cyber threats or systemic interdependencies between different critical infrastructure sectors.

We assess that some countries might be willing to explore limits on cyber operations against certain targets, although few are likely to support total bans on the development of offensive capabilities. Many countries view cyber capabilities as a useful foreign policy tool that also is integral to their domestic security, and will continue developing these capabilities. Some also remain undeterred from conducting reconnaissance, espionage, and even preparation for attacks in cyberspace.

PHYSICAL CONSEQUENCES

Our adversaries have capabilities to hold at risk U.S. critical infrastructure as well as the broader ecosystem of connected consumer and industrial devices known as the "Internet of Things." Security researchers continue to discover vulnerabilities in consumer products including automobiles and medical devices. Examples of cyber incidents with real world consequences include a cyber attack on a Ukrainian power network in 2015 that caused power outages for several hours and a "ransomware"—software designed to block a user's access to data sometimes by encrypting it—infection that forced a hospital in the United Kingdom in late 2016 to cancel scheduled medical procedures, divert trauma patients to other hospitals, and impact access to essential services such as blood transfusions. If adversaries achieve the ability to create significant physical effects inside the United States via cyber means, this would provide them new avenues for coercion and deterrence.

COMMERCIAL AND SECURITY CONSEQUENCES

Our adversaries continue to use cyber operations to undermine U.S. military and commercial advantage by hacking into U.S. defense industry and commercial enterprises in the pursuit of scientific, technical, and business information. Examples include theft of data on the F–35 Joint Strike Fighter, the F–22 Raptor fighter jet, and the MV–22 Osprey. This espionage reduces our adversaries' costs and accelerates their weapon systems development programs, enables reverse-engineering and countermeasures development, and undermines U.S. military, technological, and commercial advantage. In addition, adversaries often target personal accounts of government and industry officials as well as their close associates to enable cyber operations.

PSYCHOLOGICAL CONSEQUENCES

The impact of cyber threats extends beyond the physical, security and commercial realms. Online information operations and manipulation from both states and non-state actors can distort the perceptions of the targeted victim and other audiences through the anonymous delivery of manipulative content that seeks to gain influence or foment confusion and distrust. Information taken through cyber espionage can be leaked intact or selectively altered in content. For example, Russian actors have seeded falsified information into social media and news feeds and websites in order to sow doubt and confusion, erode faith in democratic institutions, and attempt to weaken Western governments by portraying them as inherently corrupt and dysfunctional.

CYBER POLICY, DIPLOMACY, AND WARFARE

Foreign Cyber Policies. National and domestic security interests are an important component of global Internet policy, as is a robust and stable global digital economy and the free flow of information online. As foreign countries seek to balance security, economic growth, and interoperability objectives, many are implementing new laws and technical changes to monitor and control access to information within and across their borders and to control user access through means such as restrictions on encryption and steps to reduce anonymity online.

However, these states will probably not significantly erode the overall global connectivity of the Internet. Furthermore, some state information control efforts will almost certainly be challenged by a broad coalition of states and non-state cyber stakeholders, including innovative technologists, industry leaders, privacy advocates, hackers, and others with an interest in opposing censorship or government control of cyberspace.

Diplomacy. In 2015, following a China-United States bilateral joint statement on this issue, G–20 leaders affirmed that that no country should conduct or support cyber-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors. U.S. diplomatic efforts continue to focus on the promotion of a strategic framework of international cyber stability during peacetime and during armed conflict that is built on three pillars: global affirmation of the applicability of existing international law to State activity in cyberspace; the development of international consensus on certain additional voluntary, nonbinding norms of responsible State behavior in cyberspace during peacetime; and the development and implementation of practical confidence-building measures to facilitate inter-State cooperation on cyber-related matters. The promotion of this framework is complicated by efforts to build and enhance international cooperation to address shared threats. These efforts also are hampered by the lack of consensus over key concepts such as what constitutes an armed attack, act of aggression, or the use of force in cyberspace. Furthermore, countries do not widely agree on how such principles of international law as proportionality of response or even the application of sovereignty apply in cyberspace.

Cyber Warfare. As of late 2016 more than 30 nations are developing offensive cyber attack capabilities. The proliferation of cyber capabilities coupled with new war-fighting technologies will increase the incidence of standoff and remote operations, especially in the initial phases of conflict. Cyber attacks against critical infrastructure and information networks also will give actors a means of bypassing traditional defense measures and minimizing the advantage of geography to impose costs directly on their targets from a distance. Russian officials, for example, have noted publicly that initial attacks in future wars might be made through information networks in order to destroy critically important infrastructure, undermine an enemy's political will, and disrupt military command and control. Adversaries equipped with similar offensive cyber capabilities could be prone to preemptive attack and rapid escalation in a future crisis, because both sides would have an incentive to strike first. Cyber attacks against private sector networks and infrastructure could provoke a cyber-response by the intended target, raising the possibility of corporate and other non-state actor involvement in future cyber conflict and blurring the distinction between state and non-state action. Protecting critical infrastructure, such as crucial energy, financial, manufacturing, transportation, communication, and health systems, will become an increasingly complex national security challenge.

CYBER THREAT ACTORS

Russia. Russia is a full-scope cyber actor that poses a major threat to U.S. Government, military, diplomatic, commercial, and critical infrastructure and key re-

source networks because of its highly advanced offensive cyber program and sophisticated tactics, techniques, and procedures. In recent years, we have observed the Kremlin assume a more aggressive cyber posture. Russian cyber operations targeted government organizations, critical infrastructure, think tanks, universities, political organizations, and corporations often using spearphishing campaigns. In foreign countries, Russian actors conducted damaging and/or disruptive cyberattacks, including attacks on critical infrastructure networks. In some cases Russian intelligence actors have masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. We assess that only Russia's senior-most officials could have authorized the recent election-focused data thefts and disclosures, based on the scope and sensitivity of the targets. Russia also has used cyber tactics and techniques to seek to influence public opinion across Europe and Eurasia. Looking forward, Russian cyber operations will likely target the United States to gather intelligence, support Russian decision-making, conduct influence operations to support Russian military and political objectives, and prepare the cyber environment for future contingencies.

China. Beijing continues to conduct cyber espionage against the United States Government, our allies and U.S. companies. Since the China-United States cyber commitments in September 2015, private-sector security experts continue to detect cyber activity from China, although at reduced levels and without confirmation that stolen data was used for commercial gain. Beijing has also selectively used cyber attacks against foreign targets that it probably believes threaten Chinese domestic stability or regime legitimacy. China continues to integrate and streamline its cyber operations and capabilities into a dedicated cyber element that will be increasingly difficult to detect or counter.

Iran. Tehran continues to leverage cyber espionage, propaganda, and attacks to support its security priorities, influence events and perceptions, and counter threats—including against United States allies in the Middle East. Iran has also used its cyber capabilities directly against the United States, as in distributed denial of service attacks in targeting the United States financial sector in 2012–13.

North Korea. Pyongyang remains capable of launching disruptive or destructive cyber attacks to support its political objectives, as demonstrated by its destructive attack against Sony Pictures Entertainment in 2014. South Korean officials have also concluded that North Korea was probably responsible for the 2014 compromise, exfiltration, and disclosure of data from a South Korean nuclear plant, and for numerous denial of service and data deletion attacks.

Terrorists. Terrorists groups—to include al Qaeda, Hizballah, HAMAS, and the Islamic State of Iraq and the Levant (ISIL)—continue to use the Internet to collect intelligence, coordinate operations, raise funds, spread propaganda, and incite action. Groups such as the Taliban also use Internet-based technology for similar purposes. While not as sophisticated as some state actors, Hizballah and HAMAS will continue to build on their cyber successes inside and outside the Middle East. ISIL personnel will continue to seek opportunities to target and release sensitive information about United States citizens in an effort to spur "lone-wolf' attacks as demonstrated in their 2015 operations that disclosed potential targeting information about U.S. military personnel.

Criminals. Cybercrime remains a persistent and prevalent malicious activity in cyberspace. Criminals develop and use sophisticated cyber tools for a variety of purposes including theft, extortion, and facilitation of other criminal activity. "Ransomware has become a particularly popular and effective tool for extortion, one for which few options for recovery or remediation are available if the victim has not previously backed up the affected data. In 2016, criminals employing ransomware targeted the medical sector, disrupting patient care and undermining public confidence in medical institutions. Some criminals use markets conducted on the so-called dark web to sell or lease malware to anyone willing to pay, including state and non-state actors.

RESPONSES

Perhaps the most significant counterintelligence threat to our nation, both currently and in the future, involves the rapid development and proliferation of disruptive, advanced technologies that provide adversaries with capabilities that even just a few years ago were not considered plausible. Sophisticated technical collection through a variety of means is available to more adversaries than ever before and can occur virtually anywhere and involve telephones, computers, Internet, cell phones, wired and wireless networks, as well as conversations and activities in offices, homes, vehicles, and public spaces. Disruptive technology is being built and fielded at an unprecedented rate, and we are already dealing with the consequences

of a hyperconnected world. The complexity of technological advances, both in the tools themselves and the methods used to compromise them, necessitates a much greater technical and cyber literacy than what was required of us even five years ago.

As we face this ever-changing cyber threat environment, the Intelligence Community and U.S. Cyber Command have been hardening internal U.S. Government systems, increasing knowledge and awareness among industry and the community, and engaging more closely with a host of partners to share best practices and threat information. The National Security Agency, in particular, has taken aggressive measures to hire and retain the cybersecurity talent needed to operate in this challenging environment. In addition, Cyber Command leverages the capacity and capabilities of 133 Cyber Mission Force teams that are responsible for synchronizing and executing cyber operations to support combatant command operations, and for the defense and security of service component and Department of Defense Information Networks. Cyber Command has established close working relationships with both international and interagency partners and stands ready to support a whole of nation response. The National Counterintelligence and Security Center's (NCSC) innovative public awareness campaign has resulted in placing numerous short informative videos on its public-facing website concerning cyber and associated threats, which are of immediate, practical use to federal, industry and community partners alike. NCSC also established a National Counterintelligence Task Force for Critical Infrastructure to coordinate counterintelligence efforts to mitigate this threat.

While many government organizations can make a unique contribution to securing our networks and the nation, no one agency has the capability to do so alone. The security of systems and networks is not the responsibility of one person or one agency or one industry, but rather requires a whole of nation response and a culture of cybersecurity among all users of the information space across private and public sectors.

The Intelligence Community and U.S. Cyber Command have been working to provide the Secretary of Defense and DOD policymakers with effective options for operational cyber responses to threats to U.S. interests. This remains a work in progress, and we welcome the assistance of this Committee in ensuring that we have the resources and authorities to succeed in this mission.

CONCLUSION

In summary, the breadth of cyber threats to U.S. national and economic security has become increasingly diverse, sophisticated, and dangerous. Over the next five years, technological change will only accelerate the intersection of cyber and physical devices, creating new risks. Adversaries are likely to further explore cyber-enabled psychological operations and may look to steal or manipulate data to gain strategic advantage or undermine confidence. The Intelligence Community has been vigilant in the detecting and sharing of cyber threat information with partners such as U.S. Cyber Command, as well as our nation's network protection organizations such as the Department of Homeland Security, and will continue to do so for the safety of our nation.

Chairman MCCAIN. Director, I just have to—General Clapper, I just have to mention the name, Mr. Assange, has popped up, and I believe that he is the one who is responsible for publishing names of individuals that work for us that put their lives in direct danger. Is that correct?

Director CLAPPER. Yes, he has.

Chairman MCCAIN. Do you think that there is any credibility we should attach to this individual given his record of——

Director CLAPPER. Not in my view.

Chairman MCCAIN. Not in your view.

Admiral Rogers?

Admiral ROGERS. I second those comments.

Chairman MCCAIN. Thank you.

For the record, on October 7th, the Homeland Security and Office of the Director of National Intelligence—their assessment was that the United States intelligence community is confident that the Russian Government directed the recent compromise of emails from

United States persons and institutions, including from United States political organizations. It goes on to say these thefts and disclosures are intended to interfere with the United States election process. Quote, such activity is not new to Moscow. Russians have used similar tactics and techniques across Europe and Eurasia. Quote, based on the scope and sensitivity of these efforts, only Russia's senior most officials could have authorized these activities.

General Clapper, those are still operable and correct statements?

Director CLAPPER. Yes, Chairman McCain, they are. As I indicated in my statement, we stand actually more resolutely on the strength of that statement that we made on the 7th of October.

Chairman MCCAIN. I thank you.

Really what we are talking about is if they succeeded in changing the results of an election, which none of us believe they were, that would have to constitute an attack on the United States of America because of the effects if they had succeeded. Would you agree with that?

Director CLAPPER. First, we cannot say—they did not change any vote tallies or anything of that sort. We had no way of gauging the impact that—certainly the intelligence community cannot gauge the impact it had on choices the electorate made. There is no way for us to gauge that.

Whether or not that constitutes an act of war I think is a very heavy policy call that I do not believe the intelligence community should make. But it certainly would carry in my view great gravity.

Chairman MCCAIN. Thank you.

Admiral Rogers, have you seen this problem in your position getting worse or better? In other words, it is my information that their techniques have improved, their capabilities improved. The degree of success has improved. Is that your assessment?

Admiral ROGERS. I have publicly said before that the Russians are a peer competitor in cyber. If you look broadly beyond the Russians to cyber at large, the level of capability of nation states and actors around the world continues to increase. I cannot think of a single significant actor out there who is either decreasing their level of investment, getting worse in their tradecraft or capability, or in any way backing away from significant investments in cyber.

Chairman MCCAIN. With all due respect to you, Mr. Secretary, I have not seen a policy. In other words, I do not think any of our intelligence people know what to do if there is an attack besides report it. I do not think that any of our people know, if they see an attack coming, what specific actions should be taken. Maybe I am missing something, but I have asked time after time, what do you do in the case of an attack? There has not been an answer. There has not been an answer. I believe that unless we have specific instructions to these wonderful men and women who are doing all this work, then we are going to be bystanders and observers. I am glad to hear you respond to that.

Mr. LETTRE. Mr. Chairman, you are right that we have a lot more work to do to put the right deterrence and response framework in place on cyber. This is somewhat of a new domain of operations and in some cases warfare. In my personal opinion, the next administration would be well served to focus very early on those questions of continuing to develop our overarching policy, a com-

prehensive approach, and an increasingly robust and refined deterrence framework.

Chairman MCCAIN. I thank you.

Finally, Director and Admiral, would it make your job easier if you did not have to report to seven different committees?

Director CLAPPER. Chairman McCain, my hands have been slapped before when I ventured into the delicate area of congressional jurisdiction. In the remaining 15 days that I am in office, I do not think I am going to speak to that. Afterwards that might be different.

Chairman MCCAIN. Well, we will look forward to calling you back.

[Laughter.]

Chairman MCCAIN. Admiral Rogers?

Admiral ROGERS. Can I second the comments of the Director of National Intelligence?

Chairman MCCAIN. But it does make it difficult, does it not? It is not exactly stove-piping, but overlapping jurisdictions I think makes your job a little harder, does it not, I mean in all candor, Admiral?

Admiral ROGERS. The way I would phrase is I think clearly an integrated approach is a key component of our ability to move ahead here. I would say that in the Government, in the private sector, there is no particular one slice where that is not applicable.

Chairman MCCAIN. Thank you.

Senator Reed?

Senator REED. Well, thank you very much, Mr. Chairman.

General Clapper, you responded to the chairman that in October you and the Director of Homeland Security concluded that the Russian Government intervened in the election. Admiral Rogers also seconded that view. That is also today the view, for the record, of the FBI [Federal Bureau of Investigations] and the Central Intelligence Agency [CIA], in fact, all the intelligence community. Is that correct?

Director CLAPPER. Yes. The forthcoming report is done essentially by those three agencies, CIA, FBI, and NSA.

Senator REED. The same conclusion with respect to the involvement of high-level Russian authorities is shared by all these agencies?

Director CLAPPER. Yes.

Senator REED. The chairman just noticed the legislative compartmentalization. Is that reflected also in terms of operations, in terms of, for example, Admiral Rogers, if you through NSA or through your sources detect something that is obviously a disruption, something that is patently wrong, you can communicate to the FBI or law enforcement, but there is no mechanism to make things happen administratively. Is that fair?

Admiral ROGERS. There is certainly a process, and in fact, there have been several instances that I can think of in the last 18 months where we have run through that exact same scenario. Intelligence, as it does in many other areas, other domains, will detect incoming activity of concern. We, NSA, will partner with FBI, the Department of Homeland Security, U.S. Cyber Command to en-

sure the broader government, the Department of Defense and FBI in its relationship with the private sector.

But the biggest frustration to me is speed, speed, speed. We have got to get faster. We have got to be more agile. For me at least within my span of control, I am constantly asking the team what can we do to be faster and more agile. How do we organize ourselves? What is the construct that makes the most sense? We cannot be bound by history and tradition here, so to speak. We have to be willing to look at alternatives.

Senator REED. Thank you.

General Clapper, one of the aspects of this Russian hacking was not just disseminating information that they had exploited from computers, but also the allegations of fake news sites, fake news stories that were propagated. Is that accurate, or is that one aspect of this problem?

Director CLAPPER. Yes. Without getting too far in front of the headlights of our rollout next week to the Congress, this was a multifaceted campaign. The hacking was only one part of it, and it also entailed classical propaganda, disinformation, fake news.

Senator REED. Does that continue?

Director CLAPPER. Yes.

Senator REED. The Russians particularly are very astute at covering up their tracks. It appears that they were not quite as diligent or—let me ask a question.

Do you believe that they made little attempts to cover up what they were doing as a way to make a point politically?

Director CLAPPER. Well, again, without preempting the report, that is classical tradecraft that the Russians have long used. Particularly when they are promulgating so-called disinformation, they will often try to hide the source of that or mask it to deliberately mask the source.

Senator REED. Let me just ask one more time. In this situation, though, were there attempts to mask their involvement, very elaborate and very, very sophisticated, or was it just enough to have plausible deniability?

Director CLAPPER. Sir, I would rather not get into that. That kind of edges into the sources and methods and I would rather not speak to that publicly.

Senator REED. Fair enough.

These activities are ongoing now in Europe as Europe prepares for elections. Is that a fair assumption?

Director CLAPPER. It is.

Senator REED. Thank you.

Yesterday, the "Wall Street Journal" indicated that the President-elect is considering changes to the intelligence community. Have you at all, as the experts in this field, been engaged in any of these discussions, deliberations, advice?

Director CLAPPER. No, we have not.

Senator REED. Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Inhofe?

Senator INHOFE. Thank you, Mr. Chairman.

I heard this morning that a lot of the news media was characterizing this as a hearing on Russian hacking, and actually it is on

foreign cyber threats to the United States. I am trying to cover a couple of the other ones.

First of all, I received something this morning, Director Clapper, that I was very glad to read. I have often said that the threats we are facing today are greater. I look wistfully back at the days of the Cold War. Your statement that was in print this morning said sometimes all of this makes me long for the Cold War when the world essentially had two large mutually exclusive—and so forth.

I think it is important that we talk about this because the general public is not aware of the nature of the threats that are out there that have not been out there before.

Admiral—no. Director Clapper, we have had a lot of most damaging cyber attacks perpetrated against the American people. When the chairman gave his opening statement, he singled out three or four of them. One of them was the OPM [Office of Personnel Management] incident. That was 2014 and 2015, Office of Personnel Management. It was a breach and threat to personal information, birthdates, home addresses, Social Security numbers of over 22 million individuals.

I would like to ask you what action was taken after that and what kind of effect that might have had on the behavior of the Chinese.

Director CLAPPER. Well, the major action that we took, of course, was remediation in terms of advising people of what the potential risks were. And, of course, there was a lot of work done. NSA was deeply involved in this in enhancing or improving the cybersecurity posture of OPM, and Admiral Rogers might speak to that.

I would say that this was espionage. It was not an attack per se. And, of course, I am always a bit reticent about people who live in glass houses should not throw publicly too many rocks. There is I think a difference between an act of espionage, which we conduct as well and other nations do, versus an attack.

Mike, do you want to comment?

Admiral ROGERS. Just as a broader point, I think the OPM issue highlights that massive data concentrations increasingly have value all of their own. What do I mean by that? I can remember 10 years ago earlier in my time in cyber thinking to myself large databases like OPM are so large. The ability of an intruder, an external actor to actually access, fully extract, and bore their way through millions upon millions of records would be difficult. But with the power of big data analytics, large data concentrations now become increasingly attractive targets because the ability to mine that data for insights, which is what we think drove this action in the first place, becomes more and more easily done.

Senator INHOFE. Okay. I appreciate that very much.

In your joint statement—by the way, I like the idea of joint statements. It makes our questioning a lot easier.

You talk about the—you end up stating through one of your paragraphs, in short, cyber threat cannot be eliminated. Rather, cyber threat must be managed. It is interesting that in the Edison Electric Institute—it is a publication. I think it just came in this morning—they say exactly the same thing. This seems to be one of the rare cases where we have government and industry working together. Their statement was the electric power industry recognizes

it cannot protect all assets from all threats and instead must manage risk.

Now, they go on to describe working together with government, and they say the industry's security strategy is constantly evolved and are closely coordinated with the Federal Government through a partnership called the Electricity Subsector Coordinating Council, ESCC. Can you comment? Are we looking at getting some success out of that?

Director CLAPPER. I think it is emblematic of a lot of work that the intelligence community has done, the Department of Homeland Security in engaging with each of the, I think, 16 key infrastructure sectors in this country and providing—what we have embarked on is providing them, tailored to each one of those sectors, intelligence estimates of what the threats and vulnerabilities are in order to help them take measures to enhance their cybersecurity.

I think the major point here is that if there is any connection whatsoever with the Internet, there is an inherent security vulnerability, and we have to manage the risk that is generated accordingly with full knowledge of that fact. If there is an Internet connection, there is always going to be a vulnerability.

Mike?

Admiral ROGERS. I would echo that. I think part of our challenge is our defensive strategy must be two-pronged. We have to spend time making it difficult for people to gain access, but we must acknowledge that despite our best efforts, there is a probability that they are still going to get in.

What do you do? As a guy who defends networks on the Cyber Command side, I would tell you it is a whole different process, methodology, prioritization, and risk approach in dealing with someone who is already in your network versus trying to keep them out in the first place. We have to do both.

Senator INHOFE. I appreciate that. My time has expired. I have one last question just for the record. You cannot answer it at this time.

But a year ago—it is a year and 2 months ago I think it was, Admiral Rogers—you made the statement before this committee that, quote, we have peer competitors in cyberspace and some of them have already hinted that they hold the power to cripple our infrastructure and set back our standard of living if they choose. I would like for the record if you could just kind of outline which of our peer competitors might be the closest to choosing to use their power.

Admiral ROGERS. As I have publicly said before, the Russians are the peer competitor to us. But I look at other nations. You look at China, for example, and the level of capability and investment they are making. I am watching their abilities rise significantly. Iran, North Korea, currently at a moderate level. But clearly the level of investment, the capability we are seeing, and their willingness to employ cyber in some very aggressive ways that would be way beyond our normal risk calculus is of concern.

Senator INHOFE. Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Nelson?

Senator NELSON. I think it is the general assumption that you all have said that our systems can be invaded that has the Amer-

ican people, we as policymakers concerned, but the average American concerned that there is no privacy anymore.

General, do you think in the report next week that you all will ascribe a motivation to Putin for the election attempt?

Director CLAPPER. Yes, we will ascribe a motivation. I would rather not, again, preempt the report.

Senator NELSON. Understood.

Well, then will you discuss after the report what is sufficient in the future to impose enough cost to make them stop this kind of activity?

Director CLAPPER. No. If we are going to speak to that, that would be separate from the report. What the report will include, per the President's tasking, was a section contributed by the Department of Homeland Security and NIST [National Institute of Standards and Technology], I believe, on best practices for defending, but it does not speak to that, which is really out of our lane. That is a policy call.

Senator NELSON. We are now talking about deterrence, and as one of you said in your testimony, it is not like the nuclear standoff of mutually assured destruction because we do not have a particular deterrence now. Would you discuss that?

Director CLAPPER. The point I was trying to make is that in the case of nuclear deterrence, there are instruments you can see, feel, touch, measure, weaponry. We have had a demonstration a long time ago of the impact of nuclear weaponry. That is what creates both the physical substance of deterrence, as well as the psychology. The problem with the cyber domain—it does not have those physical dimensions that you can measure, see, feel, and touch as we do with nuclear deterrence.

Senator NELSON. Let me give you an example. Help us understand had the supposed invasion into the Vermont utility been in fact an invasion by a foreign power and ascribed to that was shutting it down, if that had been the case, what would be some of the options we would do.

Director CLAPPER. Well, again, this would be a—as I understand it, by the way, it was not. But had it been from the malware planted by a foreign power, I think that is something that would be very situational dependent as to what to do about it. As I indicated in my remarks, perhaps a cyber reaction to a cyber act may not be the best course of action. Some other form of national power. Sanctions is what we have traditionally used.

As I also indicated, the problem, at least for me, is— and I will ask others to speak if they want to—if you do retaliate in a cyber context, not knowing exactly what counter-retaliation you will get back. We go through all kinds of exquisite thought processes on deciding how to react. We try to be very surgical, very precise. We try to gauge what the second order or unintended consequences might be. I do not think others are similarly disposed to consider such precision and such exactness when they respond. There is always that issue of counter-retaliation, ergo my brief mention that it is in my view best to consider all instruments of national power.

Senator NELSON. I think that is what is concerning us. Could we, the United States—do we have the ability that we could make it

so tough on North Korea with a cyber attack that it would deter them from some of their strange behavior?

Director CLAPPER. Not necessarily via a direct cyber reaction, given the difficulty of gaining access to their cyber networks.

Chairman MCCAIN. Senator Wicker?

Senator WICKER. Thank you.

Director Clapper, you are pretty far along on the report that will be released next week, obviously. How far along are you? What do you lack and how will this be released? Will it be in a classified format? Will you be willing to testify in an opening hearing like this, or will we need to go down the SCIF to hear this?

Director CLAPPER. What is planned is a series of briefings in the Congress. I think I have four more hearings to do, first with our oversight committees, which will be closed hearings I believe. Then there will be all-House, all-Senate hearings I believe next week as we roll out a version of the report——

Senator WICKER. Those will be classified.

Director CLAPPER.—followed by an unclassified version.

Senator WICKER. I see. The public will not hear sources and methods, but you think it will be fairly convincing without going beyond what——

Director CLAPPER. I assure you that I intend to push the envelope as much as I can particularly on the unclassified version because I think the public should know as much about this as possible. This is why I felt very strongly about the statement we made in October. We will be as forthcoming as we can, but there are some sensitive and fragile sources and methods here, which is one reason why we are reticent to talk about it in this setting.

Senator WICKER. You have said that, and I expect you will be challenged with some very talented questioners up and down the dais here today on that.

I would have to support what Senator Nelson has said. As regrettable and reprehensible as the hacking of political parties is, I do think Senator Nelson has touched on really the larger issue which really is the subject matter of this hearing and that is what the real threats are. It concerns me that we really do not know what the deterrence ought to be. I wonder at what level are conversations taking place within the administration or within the intelligence community about what is appropriate in terms of a response. You mentioned countering cyber with cyber is not necessarily the number one solution. Secretary Lettre mentioned that we should impose costs, and perhaps after you answer, I can ask him to expound on that also.

Director CLAPPER. Well, we have had many discussions in the White House situation room at Deputies Committee, Principals Committee, and NSC [National Security Council] meetings about what to do when we have these attacks. I think the Sony attack by the North Koreans is a case in point. There you get into the complexities of if you launch a counter cyber attack—I want to be careful here, but you have to use some other nation's infrastructure in order to mount that attack. That gets into, as I have learned, complex legal issues involving international law. The judgment was to impose some other costs other than a direct cyber retaliation.

Senator WICKER. Did you recommend the President's sanctions? Were his actions in response to the Russian hacking part of your recommendation, or did that come from someone else?

Director CLAPPER. Well, without going into internal decision-making, I think that was a consensus interagency view.

Senator WICKER. Secretary Lettre, what about imposing costs? What did you mean by that?

Mr. LETTRE. Well, as part of an approach to deterrence that takes each case as it comes up case by case, we need to look at ways to respond—first deter and then respond to attacks at a time and a place of our choosing that favors advantages that we have as we use all of the instruments available. We look to deny objectives and then impose costs, as you indicated, Senator.

Imposing costs really can come from things like were announced last week with the sanctions that were applied in the case of the Russian hacking situation, but they can go more broadly than that. From the military's perspective, we are concerned not just about Russia's cyber hacking, but also about a range of aggressive actions by Russia across multiple regions of the globe. We look to impose costs on Russia by a range of measures across multiple regions in partnership with our allies through NATO [North Atlantic Treaty Organization], where we can, to push back on Russian actions and deter future aggressive actions. That is a bit of what we mean by imposing costs here.

Senator WICKER. Thank you.

Chairman MCCAIN. It seems that every attack is handled on a case-by-case basis, and that is not a strategy.

Senator McCaskill?

Senator MCCASKILL. Thank you.

I know this will probably confuse you a little bit, General Clapper, but review again how long you have been working in intelligence.

Director CLAPPER. I started in 1963.

Senator MCCASKILL. You enlisted in 1963. Correct?

Director CLAPPER. No. I enlisted in the Marine Corps in 1961.

Senator MCCASKILL. Then transferred to the Air Force?

Director CLAPPER. Right.

Senator MCCASKILL. You flew support for combat missions in Vietnam?

Director CLAPPER. I did two tours in Southeast Asia, one in Vietnam in 1965 and 1966, and then I was stationed in Thailand flying the reconnaissance missions over Laos and Cambodia in 1970 and 1971.

Senator MCCASKILL. Would you say that your experience in the military and especially your service for the Government has always been for either political party and apolitical in terms of your mission and your job?

Director CLAPPER. Absolutely. I have served—I toiled in the trenches in intelligence for every President since President Kennedy. I have served as a political appointee in both Republican and Democratic administrations. I am apolitical.

Senator MCCASKILL. By the way, without getting into classified information, there are thousands of men and women who are work-

ing in the intelligence community right now, General Clapper. Correct?

Director CLAPPER. Absolutely.

Senator MCCASKILL. Would you say that their experience in many instances mirrors yours, in terms of military experience, many of them being either Active military or retired military?

Director CLAPPER. Yes. A large part of the intelligence community workforce are military, and of course, there are many former military, either those who completed full careers or those who served enlistments briefly and then came to the intelligence community as civilians.

Senator MCCASKILL. Would you think it any less important that we maintain the intelligence community as a foundational, apolitical bloc of our country in terms of its protection?

Director CLAPPER. I could not feel stronger about exactly that. I think it is hugely important that the intelligence community conduct itself and be seen as independent, providing unvarnished, untainted, objective, accurate, and timely and relevant intelligence support to all policymakers, commanders, diplomats, et cetera.

Senator MCCASKILL. Do, in fact, members of the intelligence community engage in life-threatening and very dangerous missions every day, particularly as it relates to the war on terror?

Director CLAPPER. You only need to walk into the lobby of CIA and look at the stars on the wall or the front lobby of NSA, and the number of intelligence people that have paid the ultimate price in the service of their country.

Senator MCCASKILL. Let us talk about who benefits from a President-elect trashing the intelligence community. Who benefits from that, Director Clapper? The American people, them losing confidence in the intelligence community and the work of the intelligence community? Who actually is the benefactor of someone who is about to become commander-in-chief trashing the intelligence community?

Director CLAPPER. I think there is an important distinction here between healthy skepticism, which policymakers, to include policymaker number one, should always have for intelligence, but I think there is a difference between skepticism and disparagement.

Senator MCCASKILL. I assume the biggest benefactors of the American people having less confidence in the intelligence community are in fact the actors you have named today, Iran, North Korea, China, Russia, and ISIS.

Director CLAPPER. The intelligence community is not perfect. We are an organization of human beings, and we are prone sometimes to make errors. I do not think the intelligence community gets the credit it is due for what it does day in and day out to keep this Nation safe and secure in the number of plots, just one example, terrorist plots that have been thwarted, both those focused on this country and other countries.

Senator MCCASKILL. I want to thank the chairman and I want to thank Senator Graham and others. There have been others I can count on maybe a little bit more than one hand who have stood up in a nonpolitical way to defend the intelligence community over the last few weeks. The notion that the soon-elected leader of this country would put Julian Assange on a pedestal compared to the

men and women of the intelligence community and the military that is so deeply embedded in the intelligence community—I think it should bring about a hue and cry no matter whether you are a Republican or a Democrat. There should be howls. Mark my word. If the roles were reversed, there would be howls from the Republican side of the aisle.

Thank you, Mr. Chairman.

Chairman MCCAIN. Thank you for that nonpartisan comment.

[Laughter.]

Chairman MCCAIN. Director Clapper, how would you describe Mr. Assange?

Director CLAPPER. How would I describe?

Chairman MCCAIN. Mr. Assange.

Director CLAPPER. Well, he is holed up in the Ecuadorian embassy in London because he is under indictment I believe by the Swedish Government for a sexual crime. He has, in the interests of ostensibly openness and transparency exposed in his prior exposures, put people at risk by his doing that. I do not think those of us in the intelligence community have a whole lot of respect for him.

Chairman MCCAIN. Admiral?

Admiral ROGERS. I would echo those comments.

Chairman MCCAIN. Thank you.

Senator Fischer?

Senator FISCHER. Thank you, Mr. Chairman.

Thank you, gentlemen, for being here today and I do thank you for your service.

Gentlemen, as you all know, about a year ago, Congress passed the Cybersecurity Information Sharing Act. Director Clapper, could you comment on what steps have been taken to implement the act in particular to provide cyber threat information in the possession of the Federal Government to non-government entities?

Director CLAPPER. There has been a lot of work done—and this is principally through both the FBI and Department of Homeland Security—to share more broadly with the private sector. Prior to the enactment of this act, I think this has been a theme that we have all worked hard. Certainly one of the reasons for the creation of the Office of Director of National Intelligence was to assume a domestic role as well and to promote sharing as much as we can. I think a lot of improvement has been made, as I look back over the last 15 years, but there is more work to do.

We have done a lot of work with, for example, fusion centers, the 76 or so fusion centers that exist throughout the country, to convey more information to them. I have a network of 12 domestic DNI [Director of National Intelligence] reps, Director of National Intelligence representatives, which are FBI special agents in charge. We work through them, those instrumentalities, on a regional basis to convey more information particularly on cyber threats to State and local officials, as well as the private sector.

Senator FISCHER. Thank you, sir.

Admiral Rogers, what is your assessment of the current state of information sharing between the Government and the private sector, especially regarding cybersecurity threats? More importantly,

what is the appropriate level of expectation to have with respect to that information sharing?

Admiral ROGERS. In some ways I would characterize it as uneven. Some sector relationships, as you heard General Clapper talk about, the 16 sectors within the critical infrastructure of our Nation—in some sectors, the relationship is very mature. Information tends to flow very regularly. Other sectors, it is not quite as mature. I think the positive side is, with the legislation, we have now developed a framework for how we do it. I still am concerned on the Government side. I will only speak for NSA and Cyber Command. On the Government side, I am not entirely comfortable that the products that I am generating are optimized to achieve outcomes for our private counterparts. I am always trying to remind our team our success needs to be defined by the customer, not what we think is the right format or the right things to share.

Senator FISCHER. Do you think there is any additional legislation that is going to be required? I guess I am asking, what do you need? Do you think there are proper authorities that are currently in place, or do we need new legislation? Or do you guys just need to improve on your execution of it?

Admiral ROGERS. Probably all of the above, to be very honest.

I look at what are the changes that we are going to need collectively to create the workforce of the future. I work within the DOD in an intel framework. But I would argue this is kind of universal. It does not matter where you are working. Where does the structure—what is the recruitment and the benefit process that we need to retain and attract a workforce?

I am curious with the new administration coming in their broad view of roles and responsibilities—are they comfortable with the current structure? Will their view be that we need to fundamentally relook at something different? I would be the first to acknowledge, as I previously said this morning, we have got to get faster. We have got to get faster.

Senator FISCHER. You know, you have talked about case by case and the ad hoc nature of our policies when it comes to cyberspace before this committee many, many times, and that has been an issue that this committee and the ETC [Emerging Threats and Capabilities] Subcommittee in particular has tried to address by requiring strategies so that we can deter these hostile actors and delegations of authority, a definition of what an act of war in cyberspace is. You know, we can go on and on. The chairman just mentioned we do not have a strategy. Some of us just do not feel there is a strategy that is laid out there.

When you talk about speed and dealing with cyber attacks, I assume you are just referring to our agencies in responding to attack that is directly upon us. Do you think there needs to be any kind of consensus-building on the international stage with our allies in order to increase speed, or would that delay it even more trying to run this through channels in trying to respond quickly? Do we reach out to allies, or do we perform our first duty in protecting this country?

Admiral ROGERS. We routinely do that now. You clearly have highlighted it is a bit of a double-edged sword. But it goes to the point from my perspective, cyber just does not recognize many of

these boundaries. When you are trying to deal with an incident, is this something that is really truly totally domestic, or has it originated from somewhere external to our Nation? What kind of infrastructure did it pass through? There is a whole lot of complexity to this. I apologize. It is not a simple binary choice there, even as I acknowledge there are tradeoffs.

Senator FISCHER. Thank you.

Thank you, Mr. Chair.

Chairman MCCAIN. Senator Blumenthal?

Senator BLUMENTHAL. Thanks, Mr. Chairman.

I want to join Senator McCaskill in expressing my appreciation for the service of our intelligence community and to you, Mr. Chairman, for your very strong and courageous statements in support of the work of this committee to give credit and credibility to that intelligence community and to your statements also about the importance of cyber warfare. It is not the first time we have been here on this topic, and you have been resolute and steadfast in seeking to elevate public awareness and public consciousness about the importance of cyber attacks on this country and the threat of cyber warfare.

I want to explore a little bit why these very demeaning and dismissive comments about our intelligence community are so dangerous to our Nation. Is it not true, Mr. Clapper, that public support for robust responses to cyber attacks on our Nation depends on the credibility of our intelligence community and dismissing the conclusions, very credible and significant conclusions, about the Russian attack undermines public support for actions that the President must take to deter and punish these kinds of actions?

Director CLAPPER. I do think that public trust and confidence in the intelligence community is crucial, both in this country and I think the dependence that other countries, other nations, have on the U.S. intelligence community. I have received many expressions of concern from foreign counterparts about the disparagement of the U.S. intelligence community or, I should say, what has been interpreted as disparagement of the intelligence community.

Senator BLUMENTHAL. Well, there is no question about the disparagement. There is no question about the dismissing and demeaning of the intelligence community, entirely unmerited. Would you agree, in light of your saying that you are even more resolute now in your conclusion about Russian involvement in this hacking, that comparing it to the judgment made about weapons of mass destruction in the Iraq situation is totally a red herring, totally wrong?

Director CLAPPER. Yes, I agree with that.

My fingerprints were on that national intelligence estimate. I was in the community then. That was 13 years ago. We have done many, many things to improve our processes, particularly with respect to national intelligence estimates, in order to prevent that from happening again.

Whatever else you want to say about the intelligence community, it is a learning organization, and we do try to learn lessons. It is a very difficult business and getting harder all the time. There will be mistakes. But what we do try to do, as we did after the NIE [National Intelligence Estimate] from October 2002 on weapons of

mass destruction in Iraq, was to learn from that, profit, and make change. Our posture, particularly with respect to a very important document, the apex of our product line, national intelligence estimates, it is the difference of night and day.

Senator BLUMENTHAL. I appreciate the extraordinary humility of that statement, especially in light of the excellence and expertise that your organization and you personally have brought to this very, very difficult endeavor to provide—and I am quoting you I think—unvarnished, untainted, timely, accurate information to the most critical national security decisions that this Nation makes. I want to express my appreciation for it and say that I think some of the disparagement has been a terrible disservice to our Nation and to the very brave and courageous men and women who put their lives at risk so that this Nation can be better informed in using our military and other force. I hope that we will see a change.

I also join the chairman in saying that we need better policies on what constitutes a cyber attack on this Nation and provide a more robust response, for example, against the Russians not necessarily in cyber but to impose stronger sanctions on their oil exports, on their use of foreign exchange. The response to cyber attacks need not be one in the cyber domain and in fact might be even more effective if it hits their economy and their pocketbook and their livelihoods.

Mr. Under Secretary, I appreciate your comments in that regard. I do not know whether you want to comment in response to what I have said. I am out of time. Maybe we can get that in writing.

Director CLAPPER. Senator Blumenthal, I do want to thank you—on behalf all the women and men of the intelligence community, I want to thank you for that.

Senator BLUMENTHAL. Thank you.

Chairman MCCAIN. Senator Cotton?

Senator COTTON. Thank you all for appearing before us.

Mr. Secretary, Director Clapper, since this is your final appearance, I know you hope, thank you very much for your many years of service, Director Clapper, particularly you.

I will add my voice to Senators Blumenthal and McCaskill in my admiration for the men and women in our intelligence agencies. I have had a chance as a member of the Intelligence Committee to meet them here at hearings and at their headquarters around the world. They do not get the credit they often deserve. The troops that we help provide for in this committee usually do because they wear uniforms and they are known in public, but intelligence officers do not wear uniforms and they are frequently undercover. I want to express my admiration and deepest respect and gratitude for what they do.

We have heard a lot of imprecise language here today—and it has been in the media as well—phrases like "hacked the election," "undermine democracy," "intervened in election." I want to be more precise here. Director Clapper, let us go to the October 7th statement. That says, quote, the recent compromises of emails from United States persons and institutions, including from United States political organizations, were instructed by the Russian Government. Are we talking there specifically about the hack of the

DNC [Democratic National Committee] and the hack of John Podesta's emails?

Director CLAPPER. Yes.

Senator COTTON. Are we talking about anything else?

Director CLAPPER. That was essentially at the time what we were talking about.

Senator COTTON. At the time then—it says that the recent disclosures through websites like DCLeaks and WikiLeaks are consistent with the methods and motivations of Russian-directed efforts. DNC emails were leaked first, I believe, in July. Is that what the statement is talking about there?

Director CLAPPER. I believe so.

Senator COTTON. Mr. Podesta's emails I believe were not leaked until that very day on October 7th. Was the statement referring to that yet, or was that not intended to be included?

Director CLAPPER. I would have to research the exact chronology of when John Podesta's emails were compromised. But I think, though, that bears on my statement that our assessment now is that is even more resolute than it was with that statement on the 7th of October.

Senator COTTON. Thank you.

Admiral Rogers, in November at the Wall Street Journal Forum, you stated, quote, this was a conscious effort by a nation state to attempt to achieve a specific effect. End quote. By that, did you also refer to the hack of the DNC, the hack of John Podesta's email and the leaks of those emails?

Admiral ROGERS. Yes.

Senator COTTON. Did you refer to anything else besides those two things?

Admiral ROGERS. To be honest, I do not remember the specifics of that one particular 30-minute engagement, but clearly what you outlined was part of my thought process.

Senator COTTON. Okay.

Then further on in that statement, Director Clapper, the intelligence community says, quote, it would be extremely difficult for someone, including a nation state actor, to alter actual ballot counts or election results by cyber attack or intrusion. End quote. You stated that earlier today as well, that we have no evidence that vote tallies were altered or manipulated in any way.

Director CLAPPER. That is correct.

Senator COTTON. That is what happened. Let us discuss why.

Director Clapper, in response to Senator Nelson, you stated that the report soon to be released will discuss the motive. Would you care to give any kind of preview today?

Director CLAPPER. I would rather not.

Senator COTTON. I did not think so.

Director CLAPPER. There is actually more than one motive. That will be described in the report.

Senator COTTON. In your 53 years of intelligence, is ascertaining the motives, plans, and intentions of foreign leaders among the hardest tasks that we ask our intelligence services to perform?

Director CLAPPER. It always has been.

Senator COTTON. There is a widespread assumption—this has been expressed by Secretary Clinton herself since the election—

that Vladimir Putin favored Donald Trump in this election. Donald Trump has proposed to increase our defense budget to accelerate nuclear modernization and to accelerate ballistic missile defenses and to expand and accelerate oil and gas production which would obviously harm Russia's economy. Hillary Clinton opposed or at least was not as enthusiastic about all those measures.

Would each of those put the United States in a strong strategic position against Russia?

Director CLAPPER. Well, certainly anything we do to enhance our military capabilities, absolutely.

Senator COTTON. There is some contrary evidence, despite what the media speculates, that perhaps Donald Trump is not the best candidate for Russia.

Okay. That is what happened. That is why it happened, or at least a preview that we are going to know why it happened. Let us move on to the impact.

Director Clapper, you said to Senator McCain earlier, quote, the intelligence community cannot gauge the impact, end quote, on the election. Is that because that kind of electoral analysis is not a task that is within the traditional responsibility and skill sets of intelligence services?

Director CLAPPER. That is correct.

Senator COTTON. That is something that is more suited for someone Shawn Hannity or Michael Barone or Nate Silver, election analysts that have written extensively on the election.

Director CLAPPER. Well, it certainly is not the purview of the U.S. intelligence community.

Senator COTTON. Thank you.

Chairman MCCAIN. Senator Heinrich?

Senator HEINRICH. Thank you, Chairman.

Since this will likely be the last hearing that some of you will attend in front of this committee, I just want to thank you all for your service and thank all the men and women who work for you. I want to say a special note of gratitude to Director Clapper for 50 years of incredible service to this country.

I think what makes America great has been our ability to elect leaders through a fair, through a peaceful and a transparent process without fear of rigging or interference in elections. Unfortunately, in this past election, we know that interference occurred. When I say "interference," I want to be specific. It is not about someone physically stuffing ballot boxes or someone hacking our electronic voting machines to give one candidate more votes than the other. It is about selectively and deliberately releasing damaging information in hopes of furthering one's strategic objectives, in this case, Russia's strategic objectives.

I believe this is going to happen again unless there is a price to be paid. This interference impacts the foundation of our democracy, our elections, which is why I welcomed the sanctions against Russia announced by the President and why I believe we need to be evaluating additional Russian sanctions. It is simply too important for both parties and for the future of our country.

Secretary Lettre, given the need for deterrence in this atmosphere which, as you said, is not always achieved by a cyber re-

sponse, how important are tools like sanctions to imposing the kind of clear costs that you articulated?

Mr. LETTRE. Sanctions are a very useful tool in that toolkit. I think in the case of the current situation that we find ourselves in, it would be prudent to continue to look at other options to impose more sanctions on Russian actors as the facts continue to develop.

Senator HEINRICH. I would agree with that estimate and I hope that folks on both sides of the aisle will be looking at those additional tools.

For any of you who want to answer this, I would like to know how has the President-elect's at least inferred dismissive attitude towards the intelligence community broadly impacted morale in your agencies?

Director CLAPPER. Well, I have not done a climate survey, but I hardly think it helps it.

Senator HEINRICH. Does anyone want to add to that?

Admiral ROGERS. I do not want to lose good, motivated people who want to help serve this Nation because they feel they are not generating value to help that Nation. I am the first to acknowledge there is room for a wide range of opinions of the results we generate. We do not question that for one minute, and every intelligence professional knows that. I have had plenty of times in my career when I have presented my intelligence analysis to commanders and policymakers, and they have just looked at me and said, hey, Mike, thanks but that is not the way I see it or you are going to have to sell me on this. That does not bother any of us. What we do I think is relevant, and we realize that what we do is in no small part driven in part by the confidence of our leaders in what we do. Without that confidence, I just do not want a situation where our workforce decides to walk because I think that really is not a good place for us to be.

Senator HEINRICH. I think many of us could not agree more. If the underlying facts that the intelligence community brings us are incorrect, we should call that out. I just have not seen any evidence indicating that in this case. Oftentimes we come to different strategic or policy points of view based on that information, but that is an entirely different thing.

Director Clapper, I want to go to a little bit more of not just the classified information, but the relevance of publicly available information of the whole picture of Russia's activities within the context of this election. Can you talk a little bit about the activities of the Russian Government's English language propaganda outlets, RT [Russian International Television], Sputnik, as well as the fake news activity we saw, as well as the social media and how those paint a complete picture that is supplemental to what we saw with the hacking in this case?

Director CLAPPER. I appreciate your raising that because while there has been a lot of focus on the hacking, this was actually part of a multi-faceted campaign that the Russians mounted. And, of course, RT, which is heavily supported, funded by the Russian Government, was very, very active in promoting a particular point of view, disparaging our system, our alleged hypocrisy about human rights, et cetera, et cetera. Whatever crack, fissure they could find in our tapestry, if you will, they would exploit it. All of these other

modes, whether it was RT, use of social media, fake news—they exercised all of those capabilities in addition to the hacking. And, of course, the totality of that I think, regardless of what the impact was which we cannot gauge, just the totality of that effort not only as DNI but as a citizen I think is of grave concern.

Senator HEINRICH. Thank you, Mr. Chair.

Chairman MCCAIN. Senator Ernst?

Senator ERNST. Thank you, Mr. Chair.

Gentlemen, thank you very much. I also want to thank you and the men and women that work diligently in the intelligence community for the work that they do for the United States of America.

Admiral Rogers, you have stated twice now—you have really stressed this point—that you must be faster and more agile in your responses. Our discussion this morning will go back to a discussion that we had in September of this last year in front of this body because I believe it is important that you understand the capabilities that exist out there and are readily available to the United States Cyber Command.

This past September, I asked you about a Government Accountability Office report that stated the Department of Defense does not have visibility of all National Guard units' cyber capabilities because the Department has not maintained a database that identifies the National Guard units' cyber-related emergency response capabilities, as required by law.

I was a bit alarmed when you stated that you have not seen the report. It was a report that took about a year to compile and was presented to both this committee and the House Armed Services Committee. Four months later, I still have not received an answer from you, my questions for the record. All of this morning, all of the GAO [Government Accountability Office] recommendations are still open from this report.

It has been 4 months and I would just like an update on that, if you have been able to read the report and where is the Department at in regards to tracking National Guard cyber capabilities?

Admiral ROGERS. Yes, ma'am. First, we did not get your question until December, but I acknowledge that you have formally asked us this.

First, as U.S. Cyber Command, I am the operational commander. Manning, training, and equipping is a function of services and the Department. For me in my role, I track the operational readiness levels of all National Guard and Reserve units that are allocated to the mission force. I bore into them in the exact same way I do the active side.

In terms of more broadly, how is the Department tracking the set of skills that are available both in the Reserve component, I would argue it is the same challenges that are in the Active component. How do you take advantage of the breadth of capability that is broader than just a particular military occupational specialty, for example? I am the first to acknowledge, after talking to my teammates at OSD and the services, I do not think we have a good answer for you. I will have something in writing for you within the next week or so because I do acknowledge that we need to do that.

Senator ERNST. I do appreciate that because how long has the United States been experiencing attacks from entities outside of the United States.

Admiral ROGERS. You could argue we have been in this cyber dynamic for over a decade. It has gotten worse.

Senator ERNST. A decade. We have taken the steps of developing Cyber Command and the capabilities that exist both in our Reserves, National Guard, and the Active component units. To become faster and more agile, we need to know what those capabilities are. If you have a solution to that on how we can track those capabilities, we need to figure that out. Many of these units have the capability of defending networks and yet we are not utilizing those capabilities. We do not know where they exist, to be honest.

Admiral ROGERS. Please do not take from my comment that we do not believe that the role of the Guard and Reserve is not important. If you look in the last 12 months, we have got two cyber protection teams from the Guard that have been mobilized. We have brought online in the Guard and the Reserve national mission teams for the first time within the last year. I mean, it is great to see how the Guard and Reserve are developing more and more capability. That is a real strength for us.

Senator ERNST. Absolutely, and I think we will continue to see those develop even more in the future, but we need to be able to utilize those capabilities that exist out there.

You know that many of our best soldiers in the National Guard and Reserve come from the private sector. I know this from some of my own guardsmen that work full-time in computer technology and cyber technology. You stated in September, you were trying to figure out how better to leverage the National Guard. Do you have a response for that? Have you thought of ways that we might be able to use those Guard units more readily?

Admiral ROGERS. This is a topic that in fact I just was talking to General Lengyel, the Director of the Guard Bureau, a few weeks ago to say, hey, look, this is something in 2017 I want us to sit down. I think there is a couple of specific mission areas where the capabilities of the Guard and Reserve are really well optimized because I would be the first to admit the answer cannot be every time we will just throw the Active component at this. I do not think that is an optimal approach for us to do in business.

You will see this play out for us in 2017. We got to work through the title 32 versus title 10 issue, what role, what is the right way to do this.

Senator ERNST. Absolutely.

Admiral ROGERS. Do we put it within the defense support to civil authority construct? I would like that because it is a framework that we already have. I am a big fan of let us not reinvent the wheel when it comes to cyber, how do we take advantage of processes and the structures and authorities that are already in place. That is one thing you will see some specific changes on within the Department. We are working through that right now on the policy side.

Senator ERNST. Very good. Well, I appreciate it. I know my time is expiring. I look forward to working with you on that, Admiral Rogers.

Chairman MCCAIN. Senator Donnelly?

Senator DONNELLY. Thank you, Mr. Chairman.

I want to thank all of you for all your efforts today, for the amazing careers you have had.

Mr. Chairman, thank you for holding this hearing. I think it is critically important to our Nation. I want to be clear that the purpose of today's hearing is not to debate the validity of the election, but to discuss foreign attempts to use cyber attacks to attack our country, including the recent Russian actions intended to influence our elections. I appreciate the bipartisan effort to get our people the answers they deserve.

I am grateful for the amazing efforts that our intelligence agencies put forth every single day, that every day lives are on the line to make sure that we are safe and to make sure that all Americans have a chance to take care of their families and go to sleep at night and not have to worry while your people are on the front lines all around the world. I can tell you on behalf all Hoosiers that when it comes down to a choice between your people, our intelligence agencies, and Julian Assange, we are on your team every time. I actually find it stunning that there is even a discussion in our country about the credibility of our intelligence agencies versus Mr. Assange. It is astounding to me that we would even make that comparison when you see the stars in the CIA headquarters of all the people who have lost their lives and all who have lost their lives in our agencies to keep us safe.

Director Clapper, how would you describe your confidence in attributing these attacks to the Russian Government as opposed to someone in their basement?

Director CLAPPER. It is very high.

Senator DONNELLY. The Government has named those responsible for the DNC hacks as APT–28 and APT–29, part of the Russian intelligence services, the GRU and the FSB [Federal Security Service]. Are all these actors targeted by these two entities known to the public, sir?

Director CLAPPER. I am sorry, sir. The question again? Were all what?

Senator DONNELLY. All the actors targeted by these two entities, the GRU, the FSB, APT–28, 29—do we know everybody? Have you told us who is involved, or are there more that you cannot discuss at this time?

Director CLAPPER. Right. I do not think I can discuss that in this forum.

Senator DONNELLY. Okay.

How far up the chain, in what you can tell us, does this go in regards to the Russians? At what level were the instructions to take these actions given?

Director CLAPPER. Again, sir, I cannot speak to that in this setting.

Senator DONNELLY. Thank you.

Do you think we are communicating clearly to our adversaries in a language that they will understand that the costs will outweigh any gains they get if they try this again? Not only you, Director, but the others, and how do we best send that message, do you think?

Director CLAPPER. Well, certainly the sanctions that have been imposed, the expulsion of the 35 intelligence operatives, the closure of the two facilities which were used for intelligence purposes, and the other sanctions that were levied, I think does convey a message. It is open to debate whether more should be done. I am a big fan of sanctions against the Russians, but that is just me.

Senator DONNELLY. Admiral, what would you say, sir?

Admiral ROGERS. I would agree. I mean, the challenge here is, look, I do not think it is in the best interest of any of our nations to be in this confrontational approach to doing business, and we have got to figure out how do we articulate what is acceptable, what is no acceptable in a way that enables us to move forward in a productive relationship. That is not unique to the Russians. I would argue that that is a challenge for us with a whole host of actors out there. This has just, in some ways, been the poster child for this challenge of late.

Director CLAPPER. I would add to that, if I may, that it certainly would be a good thing if we could find areas where our interests converge. I am speaking of ours and the Russians. We have done that in the past. Just to foot stomp Admiral Rogers' point. But I think there is a threshold of behavior that is just unacceptable, and somehow that has to be conveyed.

Senator DONNELLY. Well, I am out of time, but on behalf of all the American people, we want to thank you. You have dedicated your lives to keeping us safe, and we are incredibly grateful for it.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Sullivan?

Senator SULLIVAN. Thank you, Mr. Chairman. Thank you and the ranking member for holding this hearing.

I also want to thank you, General Clapper, Mr. Secretary, for your service, as this might be your last hearing, and the men and women you lead.

You described in your testimony the increasing attacks we are seeing not just from Russia but China and other actors, Iran, North Korea, their increasing capabilities. The chairman's opening statement pretty much stated that it is his view—and I certainly share the view—that we are being hit repeatedly because the benefits outweigh the costs for those who are taking these actions against us. Do you agree with that?

Director CLAPPER. I do and I think we all do. For adversaries like—I will just name—North Korea and Iran, it is relatively low-cost acts that can cause havoc. What I think we have seen over time is that they keep pushing the envelope because as their capabilities improve and they are willing to exercise those capabilities.

Senator SULLIVAN. If that is the case—I was glad that I think there is some consensus here. You are talking about retaliating, upping the costs with all instruments of power, Mr. Secretary, you mentioned at the time of our choosing, in the realm of our choosing. But it does not seem to be happening. It does not seem to be happening because the attacks continue.

Let me just give an example. Let us say Iran conducted—and you mentioned that they are being more aggressive more risky than North Korea—some kind of cyber attack. If we did something maybe without announcing it, like the President announced the

Russian counteraction, but let us say we did not announce it and let us say we did something where we essentially collapsed their financial system or something pretty dramatic. We let them know we did it, but we do not have to publicize it. Do you think that is the kind of action that would say, hey, do not do this or we are going to come back and retaliate at our time, our choosing, and crush you? How come we have not done that yet, and do you think if we did something like that with the Iranians or the North Koreans, would that deter them in the future, Mr. Secretary?

Mr. LETTRE. Senator, I think you are getting right at the question of what do we mean by a proportional response in some instances.

Senator SULLIVAN. Or asymmetric. You are talking about asymmetric responses, which I fully agree with.

Mr. LETTRE. That is right. Or in instances that are significantly serious and grave, whether a more than a proportional response is required to really set that deterrence framework in place.

Senator SULLIVAN. But is the key question not right now—it came from the chairman's opening statement, which I think you agreed with—is that nobody seems to be intimidated by us right now.

Let me give another example. Senator Inhofe asked a question early on about China. China hacked allegedly—maybe you can confirm that—government-led—22 million files, a lot of the SF–86 files that you use for background clearances. They have mine I was informed by the Government. Very sensitive information, as you know, that they could use against intelligence operatives and military members. Senator Inhofe asked the question, what did we do? The answer that I heard from all of you was, well, we try to protect people like me and, I am sure, others whose sensitive intel information and background information was compromised. But I did not hear any claim of a retaliation on a huge hack—huge. 22 million American Federal, military, intel workers got hacked by the Chinese.

The President signed this statement with President Xi Jinping, the United States-China Security Agreement, but obviously, General Clapper, from your testimony the Chinese have not abided by that. Have they?

Director CLAPPER. They have.

Senator SULLIVAN. I am sorry. I thought you said in your testimony today that they continue to conduct cyber attacks.

Director CLAPPER. They continue to conduct cyber espionage. They have curtailed—as best we can tell, there has been a reduction, and I think the private sector would agree with this. There has been some reduction in their cyber activity. The agreement simply called for stopping such exfiltration for commercial gain.

Senator SULLIVAN. Let me just ask a final question. Did we retaliate and up the costs against China after an enormous cyber attack against our Nation?

Director CLAPPER. We did not retaliate against an act of espionage any more than other countries necessarily have retaliated against us for when we conduct espionage.

Senator SULLIVAN. But is that answer not part of the problem that we are showing that we are not going to make it costly for

them to come in and steal the files of 22 million Americans, including many intel officers?

Director CLAPPER. Well, as I say, people who live in glass houses need to think about throwing rocks because this was an act of espionage. We and other nations conduct similar acts of espionage. If we are going to punish each other for acts of espionage, that is a different policy issue.

Chairman MCCAIN. Senator King?

Senator KING. Thank you, Mr. Chairman. Your opening statements are always erudite and thoughtful, but I thought today's was particularly so. You touched on all the important points that have really formed the basis for this hearing. I want to thank you for that.

Director Clapper, I think it is important to put some context around some of these discussions. One of the most important things to me is that your public statement in October, along with Jeh Johnson, was prior to the election, and you were simply telling facts that you had observed. In my experience of reading intelligence community communications, it is one of the more unequivocal that I have seen. You have stated here you have high confidence in those conclusions that the Russians were behind it, that it was intended to interfere with our elections, and that approval went to the highest levels of the Russian Government. Have you learned anything subsequently that you can tell us here today to contradict those findings that you publicly stated last October?

Director CLAPPER. No. In fact, if anything, what we have since learned just reinforces that statement of the 7th of October.

Senator KING. There was no political intention. You were simply reporting facts as you saw them. I presume that is correct. Your history is one of being nonpolitical.

Director CLAPPER. Absolutely. I felt particularly strongly, as did Secretary Johnson, that we owed it to the American electorate to let them know what we knew.

Senator KING. Now, people in Maine are skeptical and they want to have evidence and proof. I am hearing from people, prove it. The problem, as I understand it, is the desire to provide evidence that is convincing that your conclusions are correct versus the danger of compromising national security on sources and methods. Can you sort of articulate that? Because I think that is an important point.

Director CLAPPER. We have invested billions, and we put people's lives at risk to glean such information. If we were to fulsomely expose it in such a way that would be completely persuasive to everyone, then we can just kiss that off because we will lose it, and then that will endanger our—imperil our ability to provide such intelligence in the future. That is the dilemma that we have in intelligence. We want to be as forthcoming and transparent as possible, but we feel very, very strongly, as we do in this case, about protecting very fragile and sensitive sources and methods.

Senator KING. Let us again turn to a question of context. What we saw in this country this fall and going back actually almost a year was an example of a Russian strategy that has been playing out in Europe for some time that includes not just hacking, as you said, but disinformation, propaganda.

I heard just from a senior commander—I took a break here from the hearing—in Europe that Russia is actually buying commercial TV stations in western Europe at this point. This is a comprehensive strategy that we have seen playing out in eastern Europe, and also there was a report this morning that they are funding one of the candidates for the presidency of France in the election this May.

Director CLAPPER. Well, the Russians have a long history of interfering in elections, theirs and other people's. There is a long history in this country of disinformation. This goes back to the 1960s, you know, the heyday of the Cold War—funding that they would share or provide to candidates they supported, the use of disinformation. But I do not think that we have ever encountered a more aggressive or direct campaign to interfere in our election process than we have seen in this case.

Senator KING. There are so many more channels of disinformation today than there were in the past.

One final point.

Director CLAPPER. That is exactly right, and that is a very key point about the—of course, the cyber dimension and social media and all these other modes of communication that did not exist in the Cold War.

Senator KING. One final point. We had a meeting with the committee with a group of representatives from the Baltic States, and I know the chairman was just in the Baltic States. They are just deluged with this. I mean, they have been warning us about this for years, about the messing around with elections. I said, so what do you do? How do you defend yourself? They said, well, we are trying to defend ourselves in various ways, but the best defense is for our public to know what is going on so they can take it with a grain of salt. I thought that was a very interesting observation because their people now say, oh, yeah, that is just the Russians.

That is why I think public hearings like this and the public discussion of this issue is so important because we are not going to be able to prevent this altogether. But we need to have our people understand when they are being manipulated. Would you agree with that conclusion?

Director CLAPPER. Absolutely. That is why I felt so strongly about the statement in October.

Senator KING. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. Just to follow up, General Clapper. During the Cold War we had a strategy and we had Radio Free Europe. We had Voice of America. Senator Graham, who will be speaking next, will attest that in our recent trip they do not have a strategy. They do not have a counter-propaganda—the United States of America I am talking about. We have got to develop that strategy even if it encompasses the Internet and social media. But they are doing pretty significant stuff particularly in the Baltics and Eastern Europe. Would you agree, Senator Graham?

Senator GRAHAM. Yes. I appreciate being before the committee. Thank you.

[Laughter.]

Senator GRAHAM. Yes, I would.

Would you agree with me that Radio Free Europe is outdated?

Director CLAPPER. I am frankly not up on——

Senator GRAHAM. Well, it says "radio," and a lot of people do not listen to the radio like they used to.

Director CLAPPER. Well, actually radio is a very popular mode in many parts of the world.

Senator GRAHAM. Radio is big in your world?

Director CLAPPER. In my world?

Senator GRAHAM. Yes.

Director CLAPPER. Not so much.

Senator GRAHAM. Yes. I do not listen to the radio much either.

The bottom line is you are going to be challenged tomorrow by the President-elect. Are you okay with being challenged?

Director CLAPPER. Absolutely.

Senator GRAHAM. Do you both welcome it?

Director CLAPPER. We do.

Senator GRAHAM. Do you think it is appropriate?

Director CLAPPER. We do.

Senator GRAHAM. Are you ready for the task?

Director CLAPPER. I think so.

Senator GRAHAM. Good.

Is there a difference between espionage and interfering in an election?

Director CLAPPER. Yes. Espionage implies, to me at least, a passive collection, and this was much more activist.

Senator GRAHAM. When it comes to espionage, we better be careful about throwing rocks. When it comes to interfering in our election, we better be ready to throw rocks. Do you agree with that?

Director CLAPPER. That is a good metaphor.

Senator GRAHAM. I think what Obama did was throw a pebble. I am ready to throw a rock.

Would I be justified as a United States Senator taking your information about Russia's involvement in our election and what they are doing throughout the world and be more aggressive than President Obama if I chose to?

Director CLAPPER. That is your choice, Senator.

Senator GRAHAM. Do you think he was justified in imposing new sanctions based on what Russia did?

Director CLAPPER. I do.

Senator GRAHAM. To those of you who want to throw rocks, you are going to get a chance here soon, and if we do not throw rocks, we are going to make a huge mistake.

Admiral Rogers, is this going to stop until we make the cost higher?

Admiral ROGERS. We have got to change the dynamic here because we are on the wrong end of the cost equation.

Senator GRAHAM. Yes. You got that right.

Could it be Republicans' next election?

Admiral ROGERS. This is not about parties per se.

Senator GRAHAM. Yes. It is not like we are so much better at cybersecurity than Democrats.

Admiral ROGERS. Right.

Senator GRAHAM. Now, I do not know what Putin was up to, but I do not remember anything about Trump in the election.

Now, if Trump goes after the Iranians, which I hope he will, are they capable of doing this?

Admiral ROGERS. They clearly have a range of cyber capability and they have been willing to go offensively. We have seen in the United States in the one dam.

Senator GRAHAM. If Trump takes on China, which I hope he will, are they capable of doing this?

Admiral ROGERS. Yes.

Senator GRAHAM. We got a chance as a Nation to lay down a marker for all would-be adversaries. Do you agree with that?

Admiral ROGERS. Yes, and I would be the first to acknowledge we need to think about this broadly.

Senator GRAHAM. We should take that opportunity before it is too late.

Admiral ROGERS. Yes, sir.

Senator GRAHAM. Do you agree with me that the foundation of democracy is political parties, and when one political party is compromised, all of us are compromised?

Admiral ROGERS. Yes, sir.

Senator GRAHAM. All right.

Now, as to what to do, you say you think this was approved at the highest level of government in Russia, generally speaking. Is that right?

Director CLAPPER. That is what we said.

Senator GRAHAM. Who is the highest level of government?

Director CLAPPER. Well, the highest is President Putin.

Senator GRAHAM. Do you think a lot happens in Russia big that he does not know about?

Director CLAPPER. Not very many.

Senator GRAHAM. Yes. I do not think so.

Director CLAPPER. Certainly none that are politically sensitive in another country.

Senator GRAHAM. Okay.

Now, as we go forward and try to deter this behavior, we are going to need your support now and in the future. I want to let the President-elect know that it is okay to challenge the intel. You are absolutely right to want to do so. But what I do not want you to do is undermine those who are serving our Nation in this arena until you are absolutely sure they need to be undermined. I think they need to be uplifted, not undermined.

North Korea. Let me give you an example of real world stuff that he is going to have to deal with Trump. Do you believe that North Korea is trying to develop an ICBM [Intercontinental Ballistic Missile] to hit the United States or that could be used to hit the United States?

Director CLAPPER. That could be, yes.

Senator GRAHAM. Do you agree with that, Admiral Rogers?

Admiral ROGERS. Yes.

Senator GRAHAM. When the North Korean leader says that they are close to getting an ICBM, he is probably in the realm of truth?

Admiral ROGERS. He is certainly working aggressively to do that.

Senator GRAHAM. If the President of the United States says it will not happen, he is going to have to come to you all to figure

out how far along they are because you would be his source for how far along they are. Is that right?

Director CLAPPER. I hope we would be the source.

Senator GRAHAM. Yes. I hope he would talk to you too. Here is what I hope he realizes, that if he has to take action against North Korea, which he may have to do, I intend to support him, but he needs to explain to the American people why. One of the explanations he will give is based on what I was told by the people who are in the fight. Let me tell you this. You do not wear uniforms, but you are in the fight. We are in a fight for our lives.

I just got back from the Baltics, Ukraine, and Georgia. If you think it is bad here, you ought to go there.

Ladies and gentlemen, it is time now not to throw pebbles but to throw rocks. I wish we were not here. If it were up to me, we would all live in peace, but Putin is up to no good and he better be stopped. Mr. President-elect, when you listen to these people, you can be skeptical but understand they are the best among us and they are trying to protect us.

Thank you all.

Chairman MCCAIN. Would you have any response to that diatribe?

[Laughter.]

Director CLAPPER. Senator Graham and I have had our innings before, but I find myself in complete agreement with what he just said and I appreciate it.

Chairman MCCAIN. Thank you.

Director CLAPPER. Chairman McCain, if I might just pick up on a comment of yours and that has to do with the information fight, if you will. This is strictly personal opinion, not company policy. But I do think that we could do with having a USIA [United States Information Agency] on steroids, United States Information Agency, to fight this information war a lot more aggressively than I think we are doing right now.

Chairman MCCAIN. You know, I agree, General, and I think one of the areas where we are lacking and lagging more than any other area is social media. We know these young people in the Baltics are the same as young people here. They get their information off the Internet, and we have really lagged behind there.

Senator Gillibrand?

Senator GILLIBRAND. Thank you, Mr. Chairman and Mr. Ranking Member, for hosting this very important hearing.

I want to follow on some of the questioning that Senator Ernst started concerning the National Guard and cyber. I have been pushing DOD to use the Guard for years and appreciate that this is beginning to happen. Members of the Guard bring unique skills and capabilities, and we should be leveraging them.

Admiral Rogers, I look forward to working with you on how best to do this. Can you tell me whether there has been movement on the Army National Guard cyber protection teams being included in the cyber mission forces?

Admiral ROGERS. Yes. We brought two online that have been activated in the last year, two additional that are coming online in 2017, the first of which just came online. Yes, ma'am.

Senator GILLIBRAND. How much more is left to be done?

Admiral ROGERS. The Guard and Reserve are bringing on an additional 21 teams. Those will not be directly affiliated with the mission force. But one of the things I think we are going to find over time, the only way to generate more capacity in a resource-constrained world is to view this as an entire pie, not just, well, here is one sliced off area, the mission force, and here is a separate area, the Guard and Reserve. I think what we are going to be driven to is we are going to have to look at this as much more integrated whole.

Senator GILLIBRAND. I do too because at the end of the day, our Guard and Reserve—they have day jobs and they may be working at Google and Microsoft and Facebook and all these technology companies and have extraordinary skills. As a way to tap into the best of the best, I think we should look at people who already have these skills who are already committed to serving our Nation as best we can. I appreciate your work.

Admiral ROGERS. If I could, one area that I would be interested in your help in—for many employers in the Guard and Reserve—and I say this as the son of guardsman when I was a kid growing up—they often—sometimes—tend to view that service as something that you do overseas. Hey, I am willing to let you go because you are going to Afghanistan, you are going to Iraq. In the world of cyber, we are operating globally from a garrison, pick the location——

Senator GILLIBRAND. From any location in the world.

Admiral ROGERS. Anywhere.

This just came up. General Lengyel and I were just talking about this yesterday, as a matter of fact. I said one of the things we need to do is educate employers about what is the nature of this dynamic, and it is every bit as relevant as we are sending somebody to Afghanistan or Iraq.

Senator GILLIBRAND. I think that is right.

On a separate topic but related, I have long been advocating for aggressive development of the manpower that we need to support our cybersecurity mission. In particular, I continue to believe that we have to not only develop the capability in our military and the interest in cyber among young Americans, but that the military must be creative when thinking about recruitment and retention of cyber warriors.

How would you assess our current recruitment and retention of cyber warriors? What challenges do you foresee in the future, and what recommendations do you have to address them? Because, obviously, we are competing with some of the most dynamic, innovative companies in the world, but we need them to be our cyber defense and our cyber warriors.

Admiral ROGERS. Knock on wood. In the military aspect, we are exceeding both our recruiting and retention expectations. I worry about how long can we sustain that over time in the current model. My immediate concern is a little less on the uniform side in part because if money was a primary driver for them, they would not have come to us in the first place.

On the civilian side, however, that is probably my more immediate concern. I am finding it more challenging. We are able to recruit well. Retaining them over time—I am really running into this

on the NSA side right now. How do you retain high-end, very exquisite civilian talent for extended periods of time?

Senator GILLIBRAND. Well, I would be delighted to work with you over the next year on that.

Director Clapper, I was very interested in your opening remarks and the initial conversation you were having about the Russian hack onto the DNC and to various personnels' emails and the question of whether it was a declaration of war. Given that that is such a serious statement, I want to ask you, do you think we should take things like the Democratic or Republican Party infrastructure and consider them to be critical infrastructure? Should we actually be looking at our infrastructure differently because of this recent event?

Director CLAPPER. That has been a subject of discussion about whether, you know, our political infrastructure should be considered critical infrastructure. I know Secretary Johnson has had a discussion with State officials about that, and there is some pushback on doing that. It is a policy call. Whatever additional protections that such a declaration would afford, I think that would be a good thing. But whether or not we should do that is really not a call for the intelligence community to make.

Senator GILLIBRAND. Well, I hope it is one that the members here on this committee will discuss because if it does result in such a grave intrusion, maybe it should be critical infrastructure. Certainly politics and political parties are not set up that way, and so it would be quite a significant change.

Thank you.

Chairman MCCAIN. Director Clapper has to leave in about 20 minutes. We will enforce the time.

Senator Tillis?

Senator TILLIS. Thank you, Mr. Chair.

Gentlemen, thank you all for your service. I for one have high confidence in the community that you represent, and I hope that they recognize that I speak for most of the Senators here that share the same view.

Director Clapper, I am going to spend most my time probably reflecting on some of the comments that you have made. The glass house comment is something I think is very important.

There has been research done by a professor up at Carnegie-Mellon that has estimated that the United States has been involved in one way or another in 81 different elections since World War II. That does not include coups or regime changes. Tangible evidence where we have tried to effect an outcome to our purpose. Russia has done it some 36 times. In fact, when Russia apparently was trying to influence our election, we had the Israelis accusing us of trying to influence their election. I am not here to talk about that, but I am here to say that we live in a big glass house and there are a lot of rocks to throw. I think that is consistent with what you said on other matters.

I want to get back to the purpose of the meeting, the foreign cyber threats. I think, Admiral Rogers and Director Clapper, you all have this very difficult thing to communicate to policy people who many not have subject-matter expertise in this space. For example, Director Clapper, you were saying that one of the problems

with the counterattack—I think it was you. It could have been Admiral Rogers—is that you may have to use an asset that is actually a presence on some other nation where that nation may or may not know that we have a presence there. In fact, we have presences across cyberspace that are not known that as a part of a counterattack, the counterattack could be nothing more than exposing our presences because we know a lot of our adversaries may or may not be aware of presences that we have out there in appropriate locations. Is that correct?

Director CLAPPER. Yes, and I think you have succinctly illustrated the complexities that you run into here.

Senator TILLIS. That is why as thrilling as somebody who has written the precursors to phishing code before and stolen passwords as a part of ethical hack testings—I was paid to do this. That underscores the need for us to really be educated about the nature of this battle space and how more often than not, it is probably more prudent to seek a response that is not a cyber response given the fluid nature.

We are in an environment now where we see a threat and we build a weapon system. It is on the water. It is on the air. It is on the ground. Then we kind of counter that threat and we come up with war plans to use that capability.

In cyberspace, major weapon systems get created in 24-hour cycles. You have no earthly idea whether or not you have a defensive capability against them. If you all of a sudden think let us go declare war in cyberspace, be careful what you ask for because collectively there are 30 nations right now that have some level of cyber capability. There are four or five of them that are near peer to the United States. There are two or three that I think are very threatening and in some cases probably have superior capabilities to us in terms of presences, maybe not as sophisticated but potentially in a cyber context more lethal.

I think there are a lot of questions. One of the beauties of being a freshman—I guess now I am not a freshman—being at the end of the dais, all the good questions have been asked. But one of the things that I would suggest that we do is we as members really get educated on the nature of this threat and the manner in which we go about fighting it and understanding that the iterative nature of weapons creations on the Internet are unlike anything we have seen in record human history for warfare, and we need to understand that.

We also need to understand what the rules of engagement are going to be and how future AUMFs actually include a specific treatment for behaviors that are considered acts of war and then a whole litany of things that we should do for appropriate responses so that we can begin to make more tangible the consequences of inappropriate behavior in cyberspace.

That is not so much a diatribe, but it probably is a speech, Mr. Chair.

The last thing I will leave you with is, Admiral Rogers, I would like for my office to get with you and continue to talk about how we get these bright people, retained and recruited, to stay up to speed with developing these threats. We need to understand that they are secret to creating these weapon systems to counter the

malicious acts like Russia, China, Iran, and a number of other nations are trying to develop against us.

Thank you.

Chairman MCCAIN. Senator Hirono?

Senator HIRONO. Thank you, Mr. Chairman.

Thank you, gentlemen, for your service.

I think it is clear that we have tremendous concerns about the Russian hacking in our elections, and I think it is more than ironic that we have a President-elect who kept talking about our elections being rigged, which I would consider trying to interfere with our elections to be a part of a rigged kind of an election. At the same time, he denied Russia's activities in this regard.

Some of this was already touched on regarding the President-elect's attitudes toward the intelligence community, the impact on morale. Going forward, as we are challenged by the need to have more cyber-aware or skilled cyber workforce, if this attitude toward the intelligence community does not change on the part of decision-makers, including the President, would you agree that it would make it that much harder, Director Clapper and Admiral Rogers, to attract the kind of cyber-experienced workforce that we need to protect our country?

Director CLAPPER. Well, it could. I do not know that we could say some of these statements have had any impact on recruiting. It could.

Senator HIRONO. Or retention.

Director CLAPPER. I think it could.

On retention, I think just maybe to embellish what Admiral Rogers was saying, I do think that consideration needs to be given to having more flexibility and more latitude on compensation for our high-end cyber specialists who are lured away by industry that are paying huge salaries. That is not why you are in the Government, not why you serve in the intelligence community, not obviously for money. But I do think in those highly technical, high-end skill sets that we badly need in the Government in the intelligence community, that it would be helpful to have more latitude on compensation.

Admiral ROGERS. I would agree, Senator.

Senator HIRONO. Very briefly.

Admiral ROGERS. Both of these individuals know within the last 24 hours, which I said using my authority as the Director of NSA, I am going to authorize the following increased compensations for the high-end cyber part of our workforce because I am just watching the loss.

Senator HIRONO. Yes, of course. It is not just compensation that attracts people to what we are doing in our intelligence community because service to the country is a very important motivation. And, of course, I would think that morale would be very much attendant to that.

There was some discussion about what would constitute, in the cyber arena, an act of war. Director Clapper, I note in your testimony that I think this is one of the reasons that we want to develop international norms in this arena. Who should be the key players in developing agreeing to these international norms in the cyber arena? If the big players are United States, China, Russia,

if we do not have those players at the table to come up with these international norms, how realistic is it to develop and——

Director CLAPPER. Well, that is exactly the challenge. Those are the key nation states that we would need to engage. There has been work done under the auspices of the United Nations to attempt to come up with cyber norms, but I think we are a ways away from those having impact.

Senator HIRONO. Would you agree, Admiral Rogers?

Admiral ROGERS. Yes, ma'am.

Senator HIRONO. Turning to the awareness of the public as to the extent of the threat, a 2016 opinion piece by two members of the 9/11 Commission—basically they said that the most important thing government and leaders in the private sector can do is to clearly explain how severe this threat is and what the stakes are for the country.

Director Clapper, do you think that the general public understands the severity of the cyber threat and the stakes for the country? What should Americans keep in mind with regard to this threat? What can ordinary Americans do to contend with this threat?

Director CLAPPER. I think there is always room for more education, and certainly we have a role to play in the intelligence community in sharing as much information as we can on threats posed by both nation states, as well as non-nation states.

I think there are simple things that Americans can do to protect themselves. You know, be aware of the threat posed by spear phishing, for example, which is a very common tactic that is used yet today. We have a challenge in the Government getting our people to respond appropriately to cyber threats. This is one case where communicate, communicate, communicate is the watchword.

Chairman MCCAIN. Senator Cruz?

Senator CRUZ. Thank you, Mr. Chairman.

Gentlemen, thank you for being here. Thank you for your service to our Nation.

The topic of this hearing, cybersecurity, cyber attack, is a growing threat to this country and one that I think will only become greater in the years ahead. We have seen in recent years serious attacks from, among others, Russia, China, North Korea. Indeed, it is with some irony—I spent a number of years in the private sector, and to the best of my knowledge never had my information hacked. Then all I had

to do was get elected to the United States Senate and the Office of Personnel Management was promptly hacked and everyone on this bench had our information stolen by a foreign assault.

My question, Admiral Rogers, starting with you is what do you see as the greatest cybersecurity threats facing our country, and what specifically should we be doing about it to protect ourselves?

Admiral ROGERS. A small question.

When I look at the challenges and the threats, it is, in no particular order, significant extraction of information and insight that is generating economic advantage for others, that is eroding operational advantage at times for us as a Nation. That is, as you have seen in this Russian piece, where not just the extraction but then the use of this information adds a whole other dimension. What

concerns me beyond all that is what happens as we start to move in an environment in which not only is information being—I have heard some people use the phrase "weaponized." What happens when now we see people suddenly manipulating our networks so we cannot believe the data that we are looking at. That would be a real fundamental game-changer to me, and to me it is only a question of the "when" not the "if" this is going to happen. What happens when the non-state actor decides that cyber offers an asymmetric advantage to them? Because their sense of risk and their willingness to destroy the status quo is significantly different and greater than your typical nation state. Those are the kinds of long-term things.

As we talked about more broadly today, we have got to get better on the defensive side because part of deterrence is making it harder for them to succeed. I acknowledge that. But a defensive strategy alone is not going to work. It is a resource-intensive approach to doing business, and it puts us on the wrong end of the cost equation. That is a losing strategy for us, but it is a component of a strategy. We have got to ask ourselves how do we change this broader dynamic. To go the point you have heard repeatedly today, how do we convince nations and other actors out there that there is a price to pay for this behavior, that in fact it is not in your best interest.

Senator CRUZ. What should that price be?

Admiral ROGERS. It is a wide range of things. There is no one silver bullet, which is another point I would make. If we are looking for the perfect solution, there is not one. This will be a variety of incremental solutions and efforts that are going to play out over time. There is no one single approach here.

Senator CRUZ. Well, and your point about manipulating data, about a month ago I chaired in a different committee a hearing on artificial intelligence and our economy's growing reliance on artificial intelligence. One of the things that the witnesses testified there was concern on the cybersecurity side of a hack that would modify the big data that is being relied on for artificial intelligence to change the decision-making in a way nobody is even aware it has been changed. I think that is a threat I hope that you all are examining closely, and it is the sort of threat that could have significant repercussions without anyone even being aware it is happening.

Let me shift to a different topic. Director Clapper, you have testified before this committee that Cuba is an intelligence threat on par with Iran and listed below only Russia and China. There are reports that Lourdes, the Russian-operated signal intelligence base in Cuba, will be reopened. Additionally, this past summer Russia and Nicaragua struck a deal to increase military and intelligence cooperation, resulting in an influx of Russian tanks into Managua and an agreement to build an electronic intelligence base, which may be disguised as a satellite navigation tracking station.

To the best of your knowledge, what is Russia's strategy in the western hemisphere, and how concerned are you about the Russians expanding their influence in Cuba and Nicaragua?

Director CLAPPER. Well, the Russians are bent on establishing both a presence in the western hemisphere and they are looking for

opportunities to expand military cooperation, sell equipment, airbases, as well as intelligence gathering facilities. It is just another extension of their aggressiveness in pursuing these interests.

With respect to Cuba, Cuba has always had long-standing, very capable intelligence capabilities, and I do not see a reduction of those capabilities.

Senator CRUZ. Thank you.

Chairman MCCAIN. Senator Kaine?

Senator KAINE. Thank you, Mr. Chair.

Thanks to the witnesses for today and for your service.

Mr. Chair, I appreciate you calling this hearing. I think this hearing is a test of this body, the Article 1 branch of Congress, this hearing and others to follow.

I was chairman of the Democratic National Committee for a couple years, and we had a file cabinet in the basement that had a plaque over it. It was a file cabinet that was rifled by burglars in an invasion of the Democratic National Committee in 1972. It was a bungled effort to take some files and plant some listening devices.

That small event led to one of the most searching and momentous congressional inquiries in the history of this country. It was not partisan. One of the leaders of the congressional investigation was a great Virginian called Will Butler, who was my father-in-law's law partner in Roanoke, Virginia before he went to Congress, played a major role. It was not an investigation driven because something affected the election. The 1972 presidential election was the most one-sided in the modern era. But it was a high moment for Congress because Congress in a bipartisan way stood for the principle that you could not undertake efforts to influence an American presidential election and have there be no consequence.

The item that we will discuss and we will discuss more when the hearing comes out is different. That was a burglary of a party headquarters that was directed to some degree from the Office of the President. But this is very serious. The combined intelligence of this country has concluded that efforts were undertaken to influence an election by an adversary, an adversary that General Joe Dunford, the head of the Joint Chiefs of Staff, said in testimony before this hearing, was in his view the principal adversary of the United States at this point.

In addition, the attack was not just on a party headquarters. The October 7 letter that you have referred to talked about attacks on individuals, current and former public officials with significant positions, and also attacks on State boards of elections. The letter of October 7 traced those attacks to Russian entities, Russian companies, and did not ascribe, at least in that letter, to that directed by the Russian Government, but I am curious about what the full report will show.

It is my hope that this Congress is willing to stand in a bipartisan way for the integrity of the American electoral process and will show the same backbone and determination to get all the facts and get them on the table, as the Congress did in 1974.

There was another congressional inquiry that was directed after the attacks on 9/11, and there was a powerful phrase in that report that I just want to read. The commission concluded, quote, the most important failure was one of imagination. We do not believe

leaders understood the gravity of the threat. That is something I think we will have to grapple with. Did we have sufficient warning signs? I think we did. Having had sufficient warning signs, why did we not take it more seriously? That question is every bit as important as a question about what a foreign government, an adversary, did and how we can stop it from happening.

Three quick points.

One, is the report next week that is going to be issued not solely going to be confined to issues of hacking but also get into the dimension of this dissemination of fake news? Will that be one of the subject matters covered?

Director CLAPPER. Without preempting the report, we will describe the full range of activities that the Russians undertook.

Senator KAINE. I think that is incredibly important.

I had a little role in this election. I was along for he ride for 105 days and was the subject of a couple of fake news stories. It was interesting. There were at least three that the mainstream media did not cover because they were so incredible that like why would they. But I looked at one of the stories that had been shared 800,000 times. When I see an administration who has put in place as the proposed national security advisor someone who traffics in these fake news stories and retweets them and shares them, who betrays a sense of either gullibility or malice that would kind of be—these are stories that most fourth graders would find incredible. That a national security advisor would find them believable enough to share them causes me great concern.

Second, go back to Joe Dunford. He talked about Russia as a potential adversary because they have capacity and they have intent. With respect to our cyber, I think we have capacity, but I think what we have shown is we have not yet developed an intent about how, when, why, whether we are going to use the capacity we have. If we are going to shore up our cyber defense, in one word do you think what we really need to shore up is our capacity, or do we need to shore up our intent?

Director CLAPPER. As we look at foreign adversaries, that is always the issue is capability and intent. Certainly in the case of the Russians, they do pose an existential threat to the United States. I agree with Chairman Dunford on that. It is probably not our place, at least my place, in the intelligence community to do an assessment of our intent. That is someone else's place. It is not mine.

Chairman MCCAIN. Senator Shaheen?

Senator SHAHEEN. Thank you, Mr. Chairman and Senator Reed, for holding this hearing.

Thank you all very much for testifying this morning and for your service to the country.

Dr. Robert Kagan testified before this committee last December with respect to Russia. At that time, there was less information known to the public about what had happened in their interference in the elections.

But one of the things he pointed out was that Russia is looking at interference in elections, whether that be cyber or otherwise, the whole messaging piece that you discussed with Senator Heinrich, as another strategy along with their military action and economic and other diplomatic methods to undermine Western values, our

Euro-Atlantic alliance, and he very democracies that make up that alliance. Is that something that you agree with, Director Clapper?

Director CLAPPER. Yes. That is clearly a theme. It is certainly something that the Russians are pushing in messaging in Europe. They would very much like to drive wedges between us and Western Europe, the alliances there, and between and among the countries in Europe.

Senator SHAHEEN. I assume that there is agreement on the panel. Does anybody disagree with that?

One of the things that I think has emerged, as I have listened to this discussion, is that we do not have a strategy to respond to that kind of an effort. We do not have a strategy, it has been testified, with respect to cyber, but a broader strategy around messaging around how to respond to that kind of activity. Do you agree with that?

Director CLAPPER. I am speaking personally.

Senator SHAHEEN. Sure.

Director CLAPPER. This is not an institutional response. As I commented earlier to Senator McCain, I do think we need a U.S. Information Agency on steroids that deals with the totality of the information realm and to mount in all forums and to include the social media.

Senator SHAHEEN. I am sorry to interrupt, but can I just ask why do you believe that has not happened. Director Clapper, Admiral Rogers?

Director CLAPPER. For my part, I do not know why it has not. I cannot answer that.

Senator SHAHEEN. Admiral Rogers?

Admiral ROGERS. From my perspective, in part because I do not think we have come yet to a full recognition of the idea that we are going to have to try to do something fundamentally different. I think we still continue to try to do some of the same traditional things we have done and expecting to do the same thing over and over again, yet achieve a different result.

Senator SHAHEEN. No. That is the definition of "crazy." I think we have determined that.

Secretary Lettre?

Mr. LETTRE. I would just add that in this area, the capability and intent framework is useful to think about. I think it is only in the last few years that we have seen adversaries with true intent to use propaganda and the ability to reach out as terrorists are doing and try to incite and match that up with the tremendous power that social media tools allow to make that easy and simple and effective and broadly applicable.

Senator SHAHEEN. Given that this is a strategy and given that it is aimed not just at the United States particularly with respect to interference in our elections but at Western Europe and Eastern Europe for that matter, is there an effort underway to work with our allies through NATO or otherwise? I have been to the cybersecurity center in Estonia, but there did not seem to be a NATO agreement that this was something that we should be working on together to respond to. Is this an effort that is underway?

Mr. LETTRE. Just speaking from my lens on things, there is a lot of interest in doing that and doing it more effectively and more

comprehensively, but we have not cracked the code on doing it effectively yet. We need to keep the pressure on ourselves and our NATO allies who are likeminded in this regard to keep improving our approach.

Admiral ROGERS. It has also got to be much broader than just cyber.

Senator SHAHEEN. Thank you.

Director Clapper, my time is almost up, but before you go since this is the last opportunity we will have to hear from you, can I just ask you, do you think the DNI needs reform?

Director CLAPPER. Well, there is always room for improvement. I would never say that this is the ultimate. I do think it would be useful, though, if we are going to reform or change the DNI or change CIA, that some attention be given to, in our case, the legislative underpinnings that established the DNI in the first place and then have added additional functions and responsibilities over the years, that the Congress has added, to our kit bag of duties. But to say that there is not room for improvement, I would never suggest that.

Senator SHAHEEN. I appreciate that. I certainly agree with you. I think that if there is going to be this kind of major reform, hopefully both legislators and others who have been engaged in the intelligence community will be part of that effort.

Director CLAPPER. I certainly agree the Congress, no pun intended, gets a vote here I think.

Senator SHAHEEN. Thank you.

Chairman MCCAIN. I know that our time has expired, and I apologize to our new members that you will not have time because you have to go. But maybe, Director Clapper, since this may be, hopefully, your last appearance, do you have any reflections that you would like to provide us with, particularly the role of Congress or the lack of the role of Congress in your years of experience?

Director CLAPPER. I am going to have to be careful here.

Chairman MCCAIN. I do not think you have to be.

[Laughter.]

Director CLAPPER. I was around in the intelligence community when the oversight committees were first established and have watched them and experienced them ever since. Congress does have clearly an extremely important role to play when it comes to oversight of intelligence activities, and unlike many other endeavors of the Government, much of what we do, virtually all of what we do is done in secrecy. The Congress has a very important, a crucial responsibility on behalf of the American people for overseeing what we do particularly in terms of legality and protection of facilities and privacy.

At risk of delving into a sensitive area, though, I do think there is a difference between oversight and micromanagement.

Chairman MCCAIN. Well, we thank you. We thank the witnesses. This has been very helpful. Director Clapper, we will be calling you again.

Director CLAPPER. Really?

[Laughter.]

Chairman MCCAIN. This meeting is adjourned.

[Whereupon, at 12:09 p.m., the committee was adjourned.]

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR JAMES INHOFE

CYBER DETERRENCE

1. Senator INHOFE. Director Clapper, is it possible to deter adversaries from attacking America in an environment where the strategic capability and weapon system is available to anyone with broadband internet access?
Director CLAPPER. [Deleted.]

2. Senator INHOFE. Director Clapper, do you believe that sanctions like the ones levied against Russia in response to its election-related cyber activities are the proper tool to discourage future such behavior? What other tools would you recommend?
Director CLAPPER. [Deleted.]

3. Senator INHOFE. Director Clapper, do you believe that Obama Administration's response to Russia's recent activities represents a blueprint for effectively dealing with state-orchestrated malicious cyber activity?
Director CLAPPER. [Deleted.]

CHINA

4. Senator INHOFE. Director Clapper, do you believe China is abiding by its commitment not to support cyber enabled theft of intellectual property including trade secrets or other confidential business information for commercial advantage? Are they still conducting cyberattacks on the United States?
Director CLAPPER. [Deleted.]

TELECOM COMPANIES WITH TIES TO FOREIGN GOVERNMENTS

5. Senator INHOFE. Director Clapper, in 2012, the House Intelligence Committee determined that China-based telecommunications companies Huawei and ZTE posed potential dangers to national security due to their entanglements with the Chinese Government. The same year, Australia denied a $41-billion national broadband contract to Huawei over similar concerns. However, Huawei is again trying to making inroads in Australia, and is working in the state of Victoria on data analysis and key utility systems. Do you believe significant involvement by our close allies with companies like Huawei poses a significant threat?
Director CLAPPER. [Deleted.]

QUESTIONS SUBMITTED BY SENATOR DAVID PERDUE

THREATS TO U.S. INFRASTRUCTURE AND HOW TO RESPOND

6. Senator PERDUE. Admiral Rogers, you have stated several times that other nation states, such as Russia, China, Iran, and North Korea, have the power to cripple our critical infrastructure. Could these actors take down the U.S. power grid with their current capabilities today?
Admiral ROGERS. [Deleted.]

7. Senator PERDUE. Admiral Rogers, do such actors have the power to take down our banking and/or transportation infrastructure grids today?
Admiral ROGERS. [Deleted.]

8. Senator PERDUE. Admiral Rogers, if a state actor, or state-sponsored actor, were to take down any of our critical infrastructure (specifically, one of the 17 infrastructure subsecors designated as "critical infrastructure subsectors" by the Department of Homeland Security), would you consider this an act of war?
Admiral ROGERS. I defer to the Office of the Secretary of Defense, as the determination of what constitutes an "act of war" is a policy and legal decision. U.S. Cyber Command could respond to a Defense Support to Civil Authorities (DSCA) request if the request is routed through the Department of Homeland Security to the Secretary of Defense, and subsequently approved by the Secretary of Defense.

9. Senator PERDUE. Admiral Rogers, how would you recommend the U.S. respond to such an attack?

Admiral ROGERS. As commander of U.S. Cyber Command, I would present our Nation's leaders with suitable options for the employment of cyberspace capabilities in response to the incident, and to deter or prevent further hostile acts. However, it is important to recognize that a cyber attack does not necessarily require a cyber response. Cyber is only one element of national power our leaders can consider when developing a U.S. Government response to any type of attack on our Nation.

10. Senator PERDUE. Admiral Rogers, what are we prepared to do in response to such an attack?

Admiral ROGERS. Cyberspace response options, which vary by adversary and must be addressed on a case-by-case basis, should include whole-of-government considerations/response, and are subject to policy considerations. It is important to recognize that a cyber attack does not necessarily require a cyber response. Cyber is only one element of national power our leaders can consider when developing a U.S. Government response to any type of attack on our nation. U.S. Cyber Command's efforts to develop a rapidly maturing Cyber Mission Force (including those in the National Guard), coupled with strong relationships with intelligence organizations, foreign partners, allies, industry, academia, and joint partners, provide a resilient foundation from which we are developing cyberspace options to defend our networks, deter adversaries, and help defend the nation. U.S. Cyber Command is actively developing additional capabilities and capacities, aligned against our adversaries, so that when called upon by our nation's leaders, we are ready to support with full-spectrum cyberspace options.

DEFINITION OF CYBER "ACT OF WAR" AND INTERNATIONAL CONSENSUS

11. Senator PERDUE. Director Clapper and Admiral Rogers, you raised in your joint testimony that the key problem in dealing with cyber issues with our adversaries is that there is not an international consensus over key concpets regarding what constitutes an act of aggression or use of force in cyberspace and what international laws should govern this debate. What efforts are being undertaken to advance a sense of consensus on how we define cyberattacks on the world stage?

Director CLAPPER. [Deleted.]

Admiral ROGERS. [Deleted.]

12. Senator PERDUE. Director Clapper and Admiral Rogers, how can we better define the rules of the road for cyber internationally so we can appropriately defend our NATO allies when necessary, and so that any actions that we deem as appropriate countermeasures don't get blown out of proportion and elicit unforeseen consequences?

Director CLAPPER. [Deleted.]

Admiral ROGERS. [Deleted.]

13. Senator PERDUE. Director Clapper, you said in your February 2016 threat assessment that you would continue to monitor compliance with China's September 2015 commitment to refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property for providing a completive advantage. Could you provide us with an update on China's compliance with the September 2015 agreement?

Director CLAPPER. [Deleted.]

14. Senator PERDUE. Director Clapper, does China continue to sponsor hacking and cyber espionage for commercial gain?

Director CLAPPER. [Deleted.]

"DUAL HAT" ISSUE

15. Senator PERDUE. Admiral Rogers, in the president's signing statement of the 2017 NDAA, President Obama expressed his displeasure with the new limitations preventing the premature separation of Cyber Command and NSA. Is it still your professional military advice that maintaining the "dual hat" is in our best national security interest?

Admiral ROGERS. My professional military advice is that separation is the right step in the future, but it will take dedicated effort and resources to ensure the long-term success of both organizations following separation. Therefore, upon elevation of U.S. Cyber Command, the Commander, USCYBERCOM, should provide the Secretary of Defense and Chairman of the Joint Chiefs of Staff a vision and plan for potential future separation. This vision and plan would define the required resources and associated time table for separation.

16. Senator PERDUE. Secretary Lettre and Admiral Rogers, the President's statement suggests that the Department of Defense and the Office of the Director of National Intelligence are taking steps to begin the separation. Have you been asked to take any irreversible steps that may undermine the law the President signed a few weeks ago prohibiting the separation until a number of specific conditions have been met?

Secretary LETTRE. [Deleted.]

Admiral ROGERS. No.

17. Senator PERDUE. Admiral Rogers, how would you advise the next administration to consider the "dual hat" issue?

Admiral ROGERS. I would advise the administration that elevation and the dual-hat issue are separate and distinct. My professional military advice is that separation is the right step in the future, but it will take dedicated effort and resources to ensure the long-term success of both organizations following separation. Additionally, I recommend the elevation of U.S. Cyber Command to a combatant command occur now. Upon the elevation of U.S. Cyber Command, the Commander, U.S Cyber Command, should provide the Secretary of Defense and Chairman of the Joint Chiefs of Staff a vision and plan for potential future separation. This vision and plan would define the required resources and associated time table for separation.

ISIS—DISRUPT V. DESTROY

18. Senator PERDUE. Secretary Lettre and Admiral Rogers, according to Secretary Carter, we are "using cyber tools to disrupt ISIS's ability to operate and communicate over the virtual battlefield." Why are we only trying to "disrupt" ISIS's ability to operate and communicate in cyberspace? Shouldn't we aspire to destroy ISIS's ability to leverage cyberspace to its advantage?

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

19. Senator PERDUE. Admiral Rogers, to what extent are overly restrictive limitations or the lack of clear policy guidance from the Obama Administration impeding your ability to utilize cyber on the battlefield?

Admiral ROGERS. Cyber has been successfully used on the battlefield in support of and in executing primary military objectives; we are getting better at delivering cyber effects to support our National objectives every day. That said, it is a complex domain that requires a better coordinated whole-of-government approach and allocation of commensurate resources so that the speed at which cyber effects can be delivered meet the timing and tempo required on the battlefield. Currently, outside of existing authorities granted under the Countering Adversary Use of the Internet (CAUI) EXORD, operations that will create a cyber effect must be approved by the President (PPD–20).

20. Senator PERDUE. Admiral Rogers, how could the military better use the cyber tools at our disposal to target ISIL's ability to operate and communicate over the virtual battlefield?

Admiral ROGERS. [Deleted.]

CYBER AS A PART OF RUSSIAN HYBRID ATTACKS AND HOW TO BETTER AID EUROPEAN ALLIES

21. Senator PERDUE. Director Clapper and Secretary Lettre, we're seeing an intensification of so-called hybrid warfare by Russia not only in the United States, but also against targets in Eastern Europe, such as the use of a combination of cyberattacks, propaganda, and little green men to destabilize and otherwise subvert Ukraine. Given the fact that many of these actions can't be immediately confirmed as attributed to Russia, what's the appropriate response of nation-states to these types of actions?

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

22. Senator PERDUE. Director Clapper and Secretary Lettre, how do you think Russia might further use cyber warfare going forward to destabilize Ukraine or the Baltics, especially as a part of a broader hybrid warfare effort?

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

23. Senator PERDUE. Secretary Lettre and Admiral Rogers, what are we doing to assist states who may be vulnerable to future Russian cyberattacks to help them build up their capabilities?
Secretary LETTRE. [Deleted.]
Admiral ROGERS. [Deleted.]

24. Senator PERDUE. Director Clapper, Secretary Lettre and Admiral Rogers, how concerned should we be in the United States about the Russian capacity and capability in cyberspace?
Director CLAPPER. [Deleted.]
Secretary LETTRE. [Deleted.]
Admiral ROGERS. [Deleted.]

25. Senator PERDUE. Director Clapper and Secretary Lettre, are we prepared and postured to counter this threat?
Director CLAPPER. [Deleted.]
Secretary LETTRE. [Deleted.]

CYBER POLICY DEFICIENCIES

26. Senator PERDUE. Secretary Lettre and Admiral Rogers, some have expressed concern that the dysfunction of the White House policy process has greatly restricted the Department of Defense's ability to provide capabilities that could address urgent warfighter needs. From a warfighting standpoint, would you characterize the authorities delegated to you as being expansive or limited?
Secretary LETTRE. [Deleted.]
Admiral ROGERS. [Deleted.]

27. Senator PERDUE. Admiral Rogers, how does the delegation of authority for Cyber Command compare to the authorities you are delegated as NSA director in emergency situations?
Admiral ROGERS. [Deleted.]

28. Senator PERDUE. Admiral Rogers, how has the uncertainty hampered your ability to meet the needs of the geographic combatant commands?
Admiral ROGERS. Uncertainty in the emerging cyberspace domain is a challenge; however, close interagency coordination, information sharing, and planning has delivered positive mission outcomes in support of combatant commander objectives around the globe. As we do so, our greatest challenge is our combatant commanders want more and more as we bring forces online. I believe that is a testament to what our men and women bring to the fight. What I hear from my fellow operational commanders is "could you do even more and could you do it faster"?

IRANIAN CYBER THREATS

29. Senator PERDUE. Director Clapper, Secretary Lettre and Admiral Rogers, it now appears that Iran has ramped up its use of cyberattacks (including on U.S. financial institutions) as well as cyber reconnaissance efforts on diplomats and critical infrastructure. Do you believe that the Iranian regime has control over the majority of cyber operations that emanate from Iran? Are most cyberattacks coming from Iran state-directed?
Director CLAPPER. [Deleted.]
Secretary LETTRE. [Deleted.]
Admiral ROGERS. [Deleted.]

30. Senator PERDUE. Director Clapper, Secretary Lettre and Admiral Rogers, could you discuss Iran's cyber capabilities and how they impact our national security?
Director CLAPPER. [Deleted.]
Secretary LETTRE. [Deleted.]
Admiral ROGERS. [Deleted.]

NORTH KOREA CYBER THREATS

31. Senator PERDUE. Director Clapper, Secretary Lettre and Admiral Rogers, last year, South Korean officials uncovered a North Korean plot for a massive cyberattack where North Korea hacked into more than 140,000 computers at 160 South Korean firms and government agencies. Have you found proof of any similar

threats or attacks on United States companies and government agencies from North Korea?

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

32. Senator PERDUE. Director Clapper, Secretary Lettre and Admiral Rogers, what could be done to deter North Korean cyberattacks against the United States?

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

ADEQUATE CYBER FORCE

33. Senator PERDUE. Admiral Rogers, the Services are largely on track to meet the September 2018 goal for the training of a 6,200-person cyber force. However, the same cannot be said concerning the development and procurement of basic tools and capabilities required for both defensive and offensive cyber operations. Unless the services begin to prioritize the development of these capabilities, we could be heading down the path to a hollow cyber force. Do you agree that we are currently on the path of creating a hollow cyber force?

Admiral ROGERS. [Deleted.]

34. Senator PERDUE. Admiral Rogers, are you aware that some services failed to fund even the most basic tools like those necessary for the cyber protection teams to assess and triage compromised networks?

Admiral ROGERS. No. Each of the Services has funded its Deployable Mission Support System (DMSS) solution to support the Cyber Protection Teams. I signed the DMSS System Requirements Document (SRD) on August 16, 2016. The Services participated in the year-long drafting of the DMSS SRD and either had or were in the development of their material solution for the DMSS during SRD development. All have procured and provided—to some level—their DMSS. U.S. Cyber Command has funded and is in the process of conducting a formal assessment of each Service DMSS solution to ensure the CPTs have the minimum capability to execute their mission. Additionally, U.S. Cyber Command is drafting a TASKORD to each of the Service Cyber Components directing specific software solutions to ensure standardization to meet basic CPT requirements.

35. Senator PERDUE. Admiral Rogers, are the services committed to requesting the resources needed to make our cyber forces effective? If not, what do we need to do to ensure that we are resourcing appropriately?

Admiral ROGERS. Yes. From our perspective, each Service recognizes the needs of our cyber forces and is committed to force readiness. Each has brought capabilities to the fight for both offensive and defensive purposes. That said, because each Service uses a unique model for recruiting, organizing, manning, training, and equipping the Cyber Mission Force, we have disparate models that do not facilitate a uniform or holistic approach to force management across the DOD cyber enterprise.

Additionally, the Services continue to support most U.S. Cyber Command requests for joint capability development (manpower, tools, and infrastructure) through appropriate DOD processes.

36. Senator PERDUE. Admiral Rogers, do you have the hiring authorities needed to compete for talent with the private sector and retain them once trained?

Admiral ROGERS. [Deleted.]

QUESTIONS SUBMITTED BY SENATOR TED CRUZ

IRAN-NORTH KOREA COOPERATION

37. Senator CRUZ. Director Clapper, thank you for the response to the October 19th, 2016 letter I sent you expressing concern over the possible nuclear cooperation between Iran and North Korea. To follow up on your response, it would be helpful if you could provide input to the below questions in an unclassified format.

Director CLAPPER. [Deleted.]

38. Senator CRUZ. Director Clapper, does the Intelligence Community need any additional tools or policies to track Iranian and North Korean illicit activity?

Director CLAPPER. [Deleted.]

39. Senator CRUZ. Director Clapper, does the Intelligence Community assess that there has been a change in the level of their collaboration following Implementation Day of the JCPOA?
Director CLAPPER. [Deleted.]

40. Senator CRUZ. Director Clapper, does the Intelligence Community assess that China has increased their economic ties to North Korea, freeing the latter from some of the effects of sanctions?
Director CLAPPER. [Deleted.]

CHINA

41. Senator CRUZ. Admiral Rogers, I am concerned about the increased global reach of Chinese telecom companies that have established infrastructure in Iran, North Korea, Sudan, Syria, and now Cuba. United States intelligence agencies have linked these nominally private entities to China's military and internal Pentagon reports found that Chinese-manufactured electronics had been loaded with malware. It is my understanding the NSA, along with the FBI, has begun a formal review to assess the national security implications of a potential U.S. partnership with such a company. Can you confirm this?
Admiral ROGERS. [Deleted.]

42. Senator CRUZ. Admiral Rogers, what is your assessment of the national security risk that would result from United States firms entering joint enterprises with such Chinese telecom companies?
Admiral ROGERS. [Deleted.]

43. Senator CRUZ. Director Clapper, when China's compliance with the September 2015 cyber agreement came up in last week's hearing, you testified that China continues "to conduct cyber-espionage. They have curtailed, as best we can tell. There has been a reduction and I think the private sector would agree with this. There has been some reduction in their cyber activity. The agreement simply called for stopping such exfiltration for commercial gain." However, this reduction does not remove concern that China still seeks to appropriate United States intellectual property via cyber intrusions. According to a 2016 Department of State Overseas Security Advisory Council report, cyberattacks from Chinese hackers have continued and outpaced other nation-state actors in consistency, volume, and severity. Moreover, private firm Crowdstrike found that China continued cyberattacks on United States technology and pharmaceutical firms—suggesting a motivation to appropriate U.S. intellectual property. Despite the Intelligence Community's assessed curtailment of cyber-espionage by China, do you share the report's opinion that China remains the most active nation-state with respect to cyberattacks against American business enterprises?
Director CLAPPER. [Deleted.]

44. Senator CRUZ. Director Clapper, what level of confidence does the Intelligence Community provide their assessment that the September 2015 agreement successfully curtailed Chinese hacking and by how much has it been curtailed?
Director CLAPPER. [Deleted.]

45. Senator CRUZ. Director Clapper, does the Intelligence Community believe that the People's Republic of China has taken action against any independent cyber attackers within China?
Director CLAPPER. [Deleted.]

NORTH KOREA

46. Senator CRUZ. Director Clapper, North Korea demonstrated its cyber capabilities in the 2014 hack on Sony Pictures. In reviewing the statutory criteria of international terrorism—'violent acts or acts dangerous to human life that . . . [that] appear to be intended to intimidate or coerce a civilian population", it is my estimation that the Sony hack clearly rose to the level of coercion. In threatening Sony executives, North Korea effectively committed cyber terrorism against the United States. In your professional opinion, is the Sony hack justification for re-designating North Korea as a state sponsor of terrorism?
Director CLAPPER. [Deleted.]

QUESTIONS SUBMITTED BY SENATOR RICHARD BLUMENTHAL

NORTH KOREA

47. Senator BLUMENTHAL. Director Clapper, Secretary Lettre and Admiral Rogers, a recent report by the South Korean Defense Agency for Technology and Quality claims that North Korea possesses the capability to take down PACOM's network and inflict damage upon the United States power grid. What is your assessment of this report and North Korea's progress in development of its cyber capabilities and do you believe that they have the capacity to disrupt PACOM or the United States power system?

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

CYBERCOM

48. Senator BLUMENTHAL. Admiral Rogers, what is the timeline for elevating CYBERCOM to a fully operational combatant command?

Admiral ROGERS. I have recommended to the Secretary of Defense and the Chairman of the Joint Chiefs that Elevation of U.S. Cyber Command can occur immediately upon the decision of the President.

QUESTIONS SUBMITTED BY SENATOR ELIZABETH WARREN

U.S. TOOLS FOR CYBER RESPONSE AND STRATEGIC CALCULUS

49. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, in public remarks at a conference on November 15, 2016, Admiral Rogers described Russian-directed hacking to interfere with our election as "a conscious effort by a nation state to attempt to achieve a specific effect." The Intelligence Community's January 6, 2017 declassified report, "Assessing Russian Activities and Intentions in Recent United States Elections," [hereinafter Intelligence Community Assessment, or ICA] concluded with "high confidence" that "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the United States presidential election[,]" that "Russia's goals were to undermine public faith in the United States democratic process," and that the Russian Government's "influence campaign [. . .] blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls.'" We have a diverse array of tools in our toolbox for responding to a state-sponsored cyber-attack. The Administration exercised some of these options on December 29, 2016—expelling spies and sanctioning certain individuals and groups. When we respond to cyberattacks with our own cyber-based countermeasures, what kind of response do you generally believe is more effective: "loud" offensive actions that plainly demonstrate the strength of our capabilities to the enemy, or covert actions that might be incorrectly attributed or otherwise misinterpreted but might have a greater effect over a longer time? Please explain.

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

QUALIFICATION OF A CYBER-ATTACK AND PROTECTION OF DATA INTEGRITY

50. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, during the Committee's hearing, Director Clapper suggested a distinction between a cyber-attack and an act of cyber-espionage. Appearing before the House Intelligence Committee on September 10, 2015, Director Clapper said the July 2015 data breach of the Office of Personnel Management [hereinafter OPM] "really wasn't [an attack] since it was entirely passive and didn't result in [. . .] destruction of data or manipulation of data. It was simply stolen." If OPM employee information—or voter registration rosters in the recent election—had been manipulated or corrupted in any way, would this have constituted a cyber-attack, and what would be the threshold of intent or harm to constitute a cyber-attack? Please explain and cite any applicable legal authority or policy.

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. Whether a particular cyber activity rises to the level of an armed attack or a use of force under international law, or otherwise constitutes an unlawful intervention, is determined on a case-by-case basis by our Nation's leaders.

I defer to the Office of the Secretary of Defense response submitted below for what the threshold of intent or harm is for an action to constitute a cyber attack.

Yes. Generally, what constitutes a cyber attack is any malicious cyber activity that disrupts, denies, degrades, manipulates, or destroys computers, computer networks, the data stored on them, or the virtual or physical services and infrastructure that they support.

However, in this scenario, after a determination is made that malicious cyber activity constituted a"cyber attack" on the United States, there are a number of other factors that must be determined including attribution, the severity and impact of what is being done with the exfiltrated employee information, degree of information manipulation or corruption, and intent. Each malicious cyber activity will then be examined on a case-by-case basis and against a variety of the aforementioned factors to determine the most appropriate response. (whether the cyber activity constitutes an "armed attack" under the law of armed conflict is a slightly different question, but would similarly require a case-by-case determination in light of the scale and effects)

51. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, the potential for data manipulation is a serious concern—both for defense and civilian networks. The witnesses have previously alluded to this point in public statements. For example, in public remarks at a conference on November 19, 2015, Admiral Rogers shared concerns about data manipulation stating "what happens if what I'm looking at does not reflect reality [. . . and] leads me to make decisions that exacerbate the problem I'm trying to deal with." Our daily lives rely on confidence in the integrity of the data that is used to keep our nation safe and our economy operating. In addition to active cyber defense measures, such as firewalls, and offensive deterrence measures, do we routinely create and monitor redundancies for all critical data infrastructure such that, in the event of a breach and manipulation, we are able to positively detect and correct any distorted data? Please explain.

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

NORMS OF BEHAVIOR IN COUNTERING MALICIOUS CYBER ACTIVITY

52. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, would both state-sponsored and non-state actor-sponsored malicious cyber-attacks on the United States constitute acts of war? Please explain and cite any applicable authority.

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

53. Senator WARREN. Director Clapper and Admiral Rogers, during the Committee's hearing, USDI Lettre made a passing reference to "what do we mean by a proportional response." When the United States decides to execute countermeasures in response to malicious cyber activity that we can confidently attribute to a particular state, what are the primary considerations associated with a proportional response—the malicious nature of the cyber-attack, the unique vulnerabilities of our adversary, or other factors? Please explain and cite any applicable authority.

Director CLAPPER. [Deleted.]

Admiral ROGERS. [Deleted.]

54. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, what are the factors that determine whether malicious cyber activity—state-sponsored or committed by a non-state actor—against the United States requires a response? Please explain and cite any applicable authority.

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

55. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, how do you determine when and whether it is appropriate for the United States Government to publicly attribute malicious cyber activity directed against the United States? Please explain and cite any applicable authority.

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

56. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, how do you determine when and whether it is appropriate for the United States Government to declassify information related to a malicious cyber activity directed against the United States? Please explain and cite any applicable authority.

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. I concur with the response from Office of Secretary of Defense and defer this question to the Director of National Intelligence who is responsible for coordinating declassification determinations in accordance with Executive Order 13526.

MANAGING ESCALATION IN COUNTERING MALICIOUS CYBER ACTIVITY

57. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, how do we respond to a state-sponsored malicious cyber-attack while maintaining escalation dominance—in other words, the ability of the United States to limit the risk of unintended and prolonged escalation and end a cyber-based conflict on our terms?

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. The decision of how our Nation responds to a state-sponsored malicious cyberattack is one made by our Nation's leaders. They have all instruments of national power on the table, including other military capabilities and a whole-of-government approach as well.

As a matter of long-standing policy, we don't define how we would respond to an adversary in any domain. My duty is to provide the Secretary and President with credible options in cyberspace that, along with options in other domains, offer our leadership multiple courses of action to control escalation. From my perspective, that is best done with policies and authorities that enable our cyber mission forces to conduct their missions when directed.

ENHANCING CYBER SECURITY IN OUR DEMOCRACY

58. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, the United States has a highly-digitized, interconnected economy that is more vulnerable to cyber intrusions because the Government does not exercise authoritarian control over the Internet. How do we fortify our own critical cyber-infrastructure against attacks while maintaining the openness and transparency of our networks?

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

59. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, private businesses and other companies are increasingly the targets of state-sponsored cyber-attacks, and protecting the information held by these companies and their customers is important to our citizens' privacy, our economic security, and our national security. Cybersecurity presents many challenges, including the potential friction between information sharing among government agencies and private companies to pre-empt cyber threats, and the desire to secure communications and devices through encryption. Given the greater vulnerability of our open and interconnected networks, are you concerned that the sharing of cyber threat data among the Government and the private sector could make our country more vulnerable to theft and other malicious cyber activity—in addition to endangering the privacy of our citizens' data? Please explain, including relevant concerns under both voluntary and mandatory sharing scenarios.

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

60. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, would universal encryption—without any mandated backdoors—on servers and devices help address the unintended consequences of well-intentioned cyber threat information sharing?

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

RUSSIAN MALICIOUS CYBER ACTIVITY AGAINST OTHER NATIONS' ELECTIONS

61. Senator WARREN. Director Clapper, Secretary Lettre and Admiral Rogers, the Intelligence Community Assessment observed that Russia "will apply lessons learned from its campaign aimed at the United States presidential election to future influence efforts in the United States and worldwide, including against U.S. allies and their election processes." With elections scheduled this year in the Netherlands, France, Germany, and elsewhere, what steps are your agencies currently taking to help strengthen these and other allies' cyber defense capabilities against Russian and other election-related state-sponsored malicious cyber activity? Please explain.

Director CLAPPER. [Deleted.]

Secretary LETTRE. [Deleted.]

Admiral ROGERS. [Deleted.]

○